MultiModem® rCell

Intelligent Wireless Router

User Guide

MultiTech® Systems

MultiModem® rCell User Guide

Intelligent Wireless Router
MTCBA-H-EN2
S000456B, Revision B

Copyright

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2010 by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc., to notify any person or organization of such revisions or changes. Check Multi-Tech's Web site or product CD for current versions of our product documentation.

Record of Revisions

Revision	Date	Description
A	05/26/09	Initial release.
B	02/17/10	This release documents firmware version 2.5.

Trademarks

Trademarks and registered trademarks of Multi-Tech Systems, Inc. include MultiModem, the Multi-Tech logo, and Multi-Tech. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other products or technologies referenced in this manual are the trademarks or registered trademarks of their respective holders.

Contacting Multi-Tech Support

In order to better serve our customers, manage support requests and shorten resolution times, we have created the online web portal allowing you to submit questions regarding Multi-Tech products directly to our technical support team. Get answers to your most complex questions, ranging from implementation, troubleshooting, product configuration, firmware upgrades and much more.

To create an account and submit a Support Case on the Portal, visit support.multitech.com

Online Web Portal

support.multitech.com

The Knowledge Base provides immediate answers to your questions and gives you access to support resolutions for all Multi-Tech products. Visit our support area on the website for other support services.

Knowledge Base and Support Services

www.multitech.com/en_US/SUPPORT

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
Phone: 763-785-3500 or 800-328-9717
Fax: 763-785-9874

Technical Support

Business Hours: M-F, 9am to 5pm CST

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or (763) 717-5863

Warranty

To read the warranty statement for your product, please visit:

http://www.multitech.com/en_US/COMPANY/Policies/warranty/

Table of Contents

CHAPTER 1 – INTRODUCTION AND PRODUCT DESCRIPTION 5
MultiModem MTCBA-H-EN2 (HSDPA) 5
Safety Warnings 6
Ethernet Ports Caution 6
Handling Precautions 6
Vehicle Safety 6
Internal Lithium Battery 6
Front Panel 7
Package Contents 8
Specifications 9
RF Specifications 10
RS232 9-Pin Functions of the Female End Connector 10

CHAPTER 2 – ACTIVATION AND INSTALLATION 11
Account Activation for Wireless Devices 11
Insert the SIM Card into Holder, If required 11
Making the Connection 12
Optional – Attach the Router to a Flat Surface 13
Set Your PC's TCP/IP Address for Ethernet Functionality 14
AT Command for Verifying Signal Strength 16
AT Command for Checking Network Registration and Roaming Status 16
Configure the Ethernet Interface Using the Web Management Software 17
Shutdown Caution 19

CHAPTER 3 – USING THE WEB MANAGEMENT SOFTWARE 20
Navigating the Web Management Software 20
Web Management Software Screens 22
IP Setup 22
PPP 28
Networks & Services 34
Set Up DNAT and Port Forwarding to an Internal Device 37
GRE Tunnels 40
DHCP Server 42
IPSec 44
Add IKE Connection 45
Add Manual Connection 47
Add Manual Connection 47
Serial-Port 49
Serial-Port > Serial Port Settings 49
Serial Port > Server Settings 51
Tools 52
Tools > Save Configuration 53
Statistics & Logs 54
Statistics & Logs > System Information 54
Statistics & Logs > Ethernet 55
Statistics & Logs > PPP 56
Statistics & Logs > PPP Trace 57
Statistics & Logs > GRE Statistics 57
Statistics & Logs > Modem Information 58
Statistics & Logs > Service Status 58
Statistics & Logs > TCP/UDP Client Live Log 58
Statistics & Logs > TCP/UDP Server Live Log 58
Statistics & Logs > IPSec Live Log 59
Statistics & Logs > IPSec Log Traces 59

APPENDIX A – A REFERENCE TABLE OF COMMONLY SUPPORTED SUBNETS 60

APPENDIX B – WIRELESS ANTENNA 62
GSM/EGSM Antenna Requirements/Specifications 62
Antennas Available from Multi-Tech Systems, Inc. 62
PTCRB Requirements Note: 62
FCC Requirements Note: 62
GSM and E-GSM Radio Characteristics 62

APPENDIX C – REGULATORY COMPLIANCE 63
EMC, Safety, and R&TTE Directive Compliance 63

FCC Part 15 Class A Statement....63
Industry Canada....63
APPENDIX D – WASTE ELECTRICAL AND ELECTRONIC EQUIPMENT....64
APPENDIX C – ROHS HT/TS SUBSTANCE CONCENTRATION....65
INDEX....66

Chapter 1 – Introduction and Product Description

This User Guide describes the MultiModem® rCell, model MTCBA-H-EN2, Intelligent Wireless Router with an Ethernet 2 interface. The MultiModem rCell Router configured for one of three connectivity modes: always-on, wake-up on ring, or dial-on demand. The always-on network connection automatically establishes a wireless data connection and allows for around the clock surveillance, monitoring or real time data acquisition of any remote Ethernet device such as a Web camera. If the data link is dropped in the event of poor reception or a complete loss of service, it will automatically re-establish the data link. The wake-up on ring configuration allows the router to "wake up" and initiate a connection when it detects an incoming ring. For security reasons, you can setup the router to wake up based on a particular caller ID number. This configuration is ideal for reducing the costs associated with the modem being online and available 24/7. When configured for dial-on demand, the router only accesses the Internet when data is present. This configuration is ideal for sharing Internet access among networked PCs.

MultiModem MTCBA-H-EN2 (HSDPA)

The MultiModem MTCBA-H-EN2 wireless router delivers some of the fastest cellular data speeds by utilizing HSDPA technology. It allows users to connect to the Internet and send and receive data faster than possible with an ordinary GSM/GPRS network making it ideal for highly data-intensive applications. Based on industry-standard open interfaces, the MultiModem MTCBA-H-EN2 wireless router is equipped with quad-band, high-speed RS232 technology, which means it can be used worldwide on all existing GSM networks.

AT Commands: The MultiModem MTCBA-H-EN2 wireless router is configured using the HSDPA AT Commands. These commands are documented in the Reference Guide for the MultiModem Wireless HSDPA Router, document number S000453*x*.

Safety Warnings

Ethernet Ports Caution

The Ethernet ports are **not** designed to be connected to a Public Telecommunication Network or used outside the building.

Handling Precautions

All devices must be handled with certain precautions to avoid damage due to the accumulation of static charge. Although input protection circuitry has been incorporated into the devices to minimize the effect of this static build up, proper precautions should be taken to avoid exposure to electrostatic discharge during handling and mounting.

Caution: Maintain a separation distance of at least 20 cm (8 inches) between the transmitter's antenna and the body of the user or nearby persons. The router is not designed for, nor intended to be, used in applications within 20 cm (8 inches) of the body of the user.

Vehicle Safety

- Do not use your Router while driving, unless equipped with a correctly installed vehicle kit allowing 'Hands-Free' Operation.
- Respect national regulations on the use of cellular telephones in vehicles. Road safety always comes first.
- If incorrectly installed in a vehicle, the operation of router telephone could interfere with the correct functioning of vehicle electronics. To avoid such problems, be sure that qualified personnel have performed the installation. Verification of the protection of vehicle electronics should be part of the installation.
- The use of an alert device to operate a vehicle's lights or horn on public roads is not permitted.

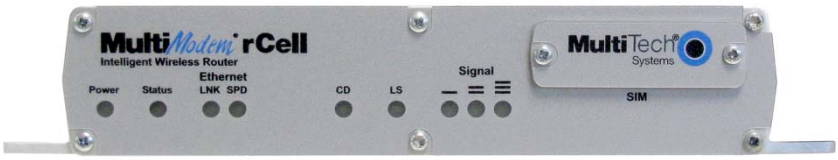
Internal Lithium Battery

- A lithium battery located within product provides backup power for the timekeeping capability. The battery has an estimated life expectancy of ten years.
- When the battery starts to weaken, the date and time may be incorrect. If the battery fails, the board must be sent back to Multi-Tech Systems for battery replacement.
- Lithium cells and batteries are subject to the Provisions for International Transportation. Multi-tech Systems Inc. confirms that the Lithium batteries used in the Multi-Tech product(s) referenced in this manual comply with **Special Provision 188 of the UN Model Regulations**, **Special Provision A45 of the ICAO-TI/IATA-DGR (Air)**, **Special Provision 310 of the IMDG Code**, and **Special Provision 188 of the ADR and RID (Road and Rail Europe)**.

  Warning! There is danger of explosion if the battery is incorrectly replaced!

Front Panel

The front panel contains Power and Status LEDs, two Ethernet LEDs, two modem LEDs, and three signal LEDs. The Power LED indicates that DC power is present and the Status LED blinks when the unit is functioning normally. The two Ethernet LEDs indicate transmit and receive activity and connection speed of 10 or 100Mbps on the Ethernet link. The two modem LEDs indicate carrier detection and link status. The three signal LEDs display the signal strength level of the wireless connection. The SIM door on the right side of the router provides access to the SIM card holder.



LED Indicators	
Power	Indicates presence of DC power when lit.
Status	The LED is a solid light when the rCell is booting up, saving the configuration, restarting, or updating the firmware. When the Status LED begins to blink, the router is ready.
LNK	**Link.** Blinks when there is transmit and receive activity on the Ethernet link. It shows a steady light when there is a valid Ethernet connection.
SPD	**Speed.** Lit when the Ethernet is linked at 100 Mbps. If it is not lit, the Ethernet is linked at 10 Mbps.
CD	**Carrier Detect.** Lit when data connection has been established.
LS	**Line Status.** **Continuous "on" state** indicates that the wireless modem is registered on the network. **Flashing state** Indicates attempted registration on network. **Off state.** Modem could not register
Signal	**ALL OFF -** Unit is off, not registered on network, or extremely week signal (0 < = RSSI < 6). **1 Bar** "**ON**" – Very weak signal (7 < = RSSI <14) **1 Bar** and **2 Bar** "**ON**" – Weak signal (15 < = RSSI <23) **1 Bar**, **2 Bar**, and **3 Bar** "**ON**" – Good signal (24 <= RSSI > = 31)

Package Contents

Unbundled Package with No Accessories	Bundled Package with Accessories
1 router 1 Quick Start Guide 1 MultiModem CD **Note:** You must supply mounting screws, AC or DC power supply, and an antenna.	1 router 1 antenna 1 Ethernet cable 1 RS-232 cable 1 power supply 1 Quick Start Guide 1 MultiModem CD **Note**: You must supply mounting screws.

Note: Your wireless provider will supply the SIM card.

Specifications

Performance	**HSDPA/UMTS, EDGE:** Class 10, **GPRS;** Class 10
Band, Frequency	Quad-band, GSM/GPRS/EDGE/HSDPA, 850/900/1800/1900 MHz, UMTS FDD: Band I/Band II/Band V
Packet Data	**HSDPA:** UE CAT [1-6], 11, 12 supported, compressed mode according to 3GPP TS5.212 **EDGE:** Class 10, full PBCCH support, coding schemes CS-9, Mobile station Class B **GPRS:** Class 10, full PBCCH support, coding schemes CS1-4, Mobile station Class B
Circuit-Switched Data	**GSM:** Asynchronous, non-transparent up to 9600bps **UMTS:** Asynchronous,non- transparent up to 64K bps
Short Message Services-SMS	Text & PDU,Point-to-Point (MO/MT), cell broadcast
Antenna Connector	RF Antenna: 50 ohm SMA (female connector)
SIM Connector	Standard 1.8 & 3V SIM receptacle
RS232 Connector	DE9
Power Connector	2.5mm miniature(screw-on)
Voltage	9V to 32 VDC @1.44A
Power*	**Sleep** .180A, 1.665W @ 9V, .092A, 1.84W @ 20V, .061A, 1.958W @32V **Typical** .480A, 4.382W @ 9V, .230A, 4.60W @ 20V, .0150A, 4.80W @32V **Max** .665A, 6.025W @ 9V, .310A, 6.175W @ 20V, .200A, 6.40W @ 32V
Physical Description	7” W x 1.24”H x 2.79”D .78lbs 17.78 cmW x3.15cmH x 7.07cmD .355Kg
Operating Temperature **	-30° to +60° C UL listed @ 40°
Storage Temp	-40° to +85° C
Humidity	Relative humidity 20% to 90% noncondensing
Certifications	**CE Mark, R&TTE** **EMC Compliance** FCC Part 15 EN55022 EN55024 **Radio Compliance** FCC Part 22, 24 RSS 132,133,102 EN301 489-1 EN301 489-7 EN301 511 **Safety:** UL60950-1 cUL60950-1 IEC60950-1 AS/NZS60950-1 **Network:** PTCRB

* Multi-Tech Systems, Inc recommends that the customer incorporate a 10% buffer into their power source when determining product load.

** UL Listed @ 40°C. Limited by power supply. UL Certification does not apply or extend to an ambient above 40°C and has not been evaluated by UL for ambient greater than 40°C

“UL has evaluated this device for use in ordinary locations only. Installation in a vehicle or other outdoor locations has not been evaluated by UL. UL Certification does not apply or extend to use in vehicles or outdoor applications or in ambient above 40° C.”

Optional power must be UL Listed ITE power supply marked LPS or Class 2 rated 9-32Vdc, 1.44 – 0.4A

RF Specifications

	GSM 850	EGSM 900	GSM 1800	GSM 1900
Frequency RX	869 to 894 MHz	925 to 960 MHz	1805 to 1800 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz
RF Power Stand	2W at 12.5% duty cycle	2W at 12.5% duty cycle	1W at 12.5% duty cycle	1W at 12.5% duty cycle

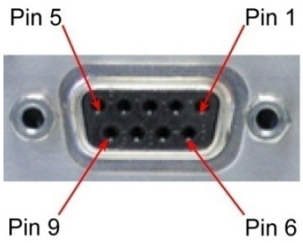
RS232 9-Pin Functions of the Female End Connector

The following table explains the pin functions.

External Power	
Signal	**IN/OUT**
Pin 1 CD	O
Pin 2 RX	O
Pin 3 TX	I
Pin 4 DTR	I
Pin 5 GND	--
Pin 6 DSR	O
Pin 7 RTS	I
Pin 8 CTS	O
Pin 9 RI	O

Serial Cable

Female Connector



Chapter 2 – Activation and Installation

Account Activation for Wireless Devices

Please refer to the wireless account Activation Notice included with your unit and located on the MultiModem CD. Follow the directions on the Activation Notice to activate your account.

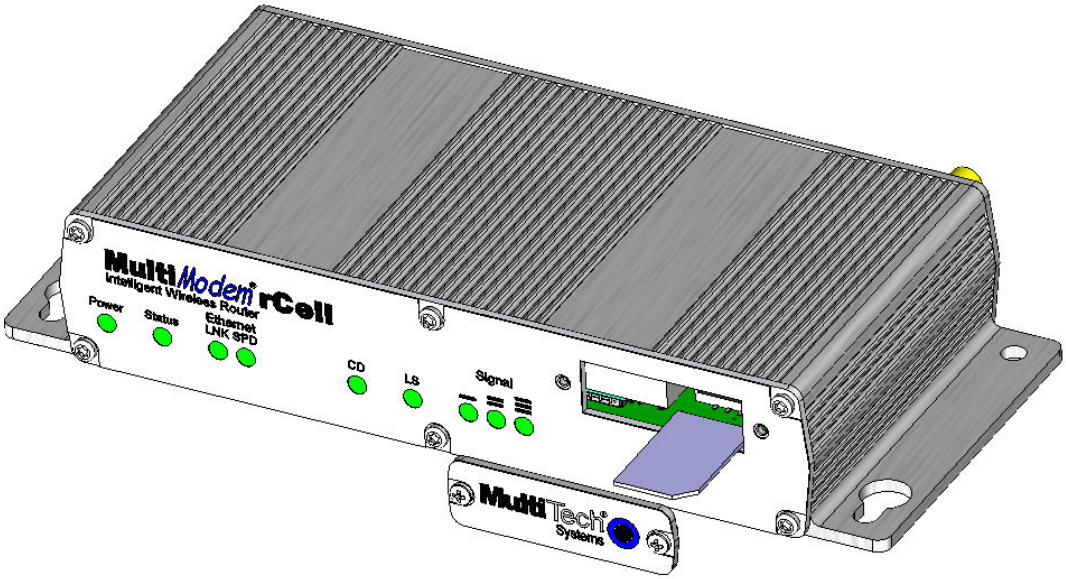
Note: If you need remote access to your MultiModem over the Internet for remote configuration, you need to ensure that your wireless network provider has provisioned mobile terminated data and fixed or dynamic public IP address in which they can configure the network to redirect any incoming connection to that predefined IP.

Insert the SIM Card into Holder, If required

The router requires the power supply connection to begin operation. It also requires a SIM card (Subscriber Identity Module) to operate on a GSM network. To install the SIM, do the following:

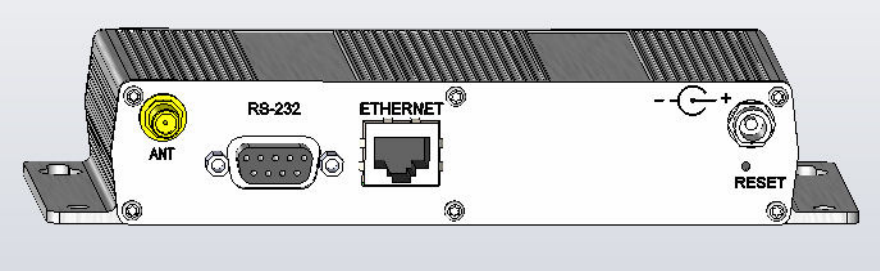
1. Using a small Phillips screwdriver, remove the two SIM door screws and remove the SIM door.

   Note: When changing a SIM, ensure that power is removed from the unit.

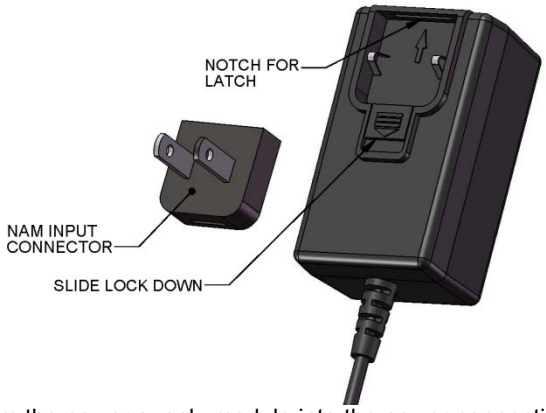


2. Insert the SIM card into the card holder. The above graphic illustrates the correct SIM card orientation.
3. Verify that the SIM card fits into the holder properly and then replace the cover.

Making the Connection



1. Connect a suitable antenna to the SMA connector (see antenna specifications in Appendix B).
2. Using an Ethernet cable, connect one end of the cable to the ETHERNET connector on the back of the router and the other end to your pc either directly or via a switch or hub.
3. If you are connecting a customer's serial legacy device to the router, connect the serial, RS-232 cable from the customer's device to the RS232 connector on the back of the router.
4. Depending on the power source, connect either the power supply module with the appropriate blade or the optional DC power cable. If you are using the power supply module, remove the protective shipping cover. Attach the appropriate interchangeable blade piece to the power supply module.



5. Screw-on the power lead from the power supply module into the power connection on the router. Now, plug the power supply into your power source.

For Optional Direct DC Power

- Screw-on the DC power cable to the power connector on the router.
- Then attach the two wires at the other end of the DC power cable to a DC fuse/terminal block in which you are mounting the router.
- Connect red wire to the "+" (positive) terminal and black wire to the "–" (negative) terminal. Be sure the GND connection is correct.

Warning: Over-voltage protection is provided on the device. To ensure complete protection, you may want to add additional filtering to the DC input.

Note: For an application involving a battery: you can use permanent "+" or key-switched "+" source. Connect the power supply to its source (for example, in a mobile situation, to the DC fuse/terminal block).

Notes

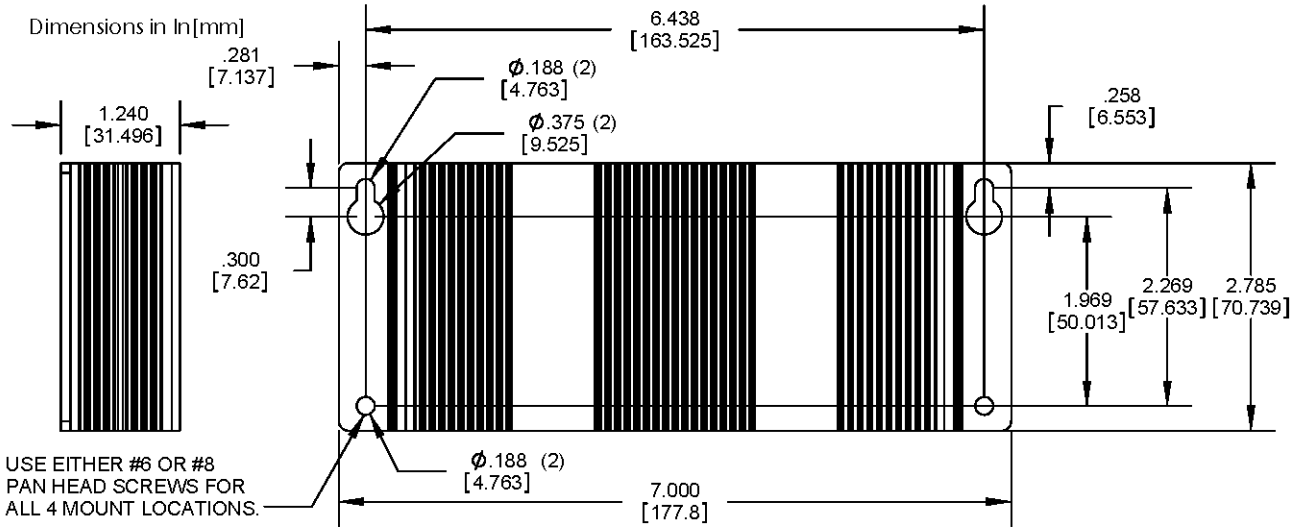
- The **POWER** LED**.** The **POWER** LED lights after power-up.
- The **Status** LED is a solid ON when the router is booting up, saving a configuration, or updating firmware. When the **Status** LED begins to blink, the router is ready.
- The **Reset** Button**.** Pressing and holding the **Reset** button for 5 seconds will restore all factory default settings. It also will set the username and password back to admin and admin as well as setting the IP address to the default of 192.168.2.1.

Optional – Attach the Router to a Flat Surface

Before you mount your router to a permanent surface, verify signal strength, refer to Verify Signal Strength in this Chapter.

The router can be panel mounted with screws spaced according to the measurement shown.

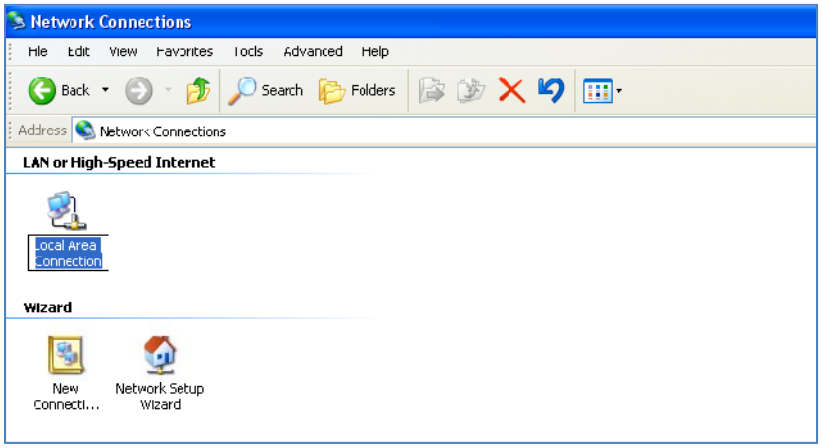
Note: Use either #6 or #8 pan head screws for all four mount locations.



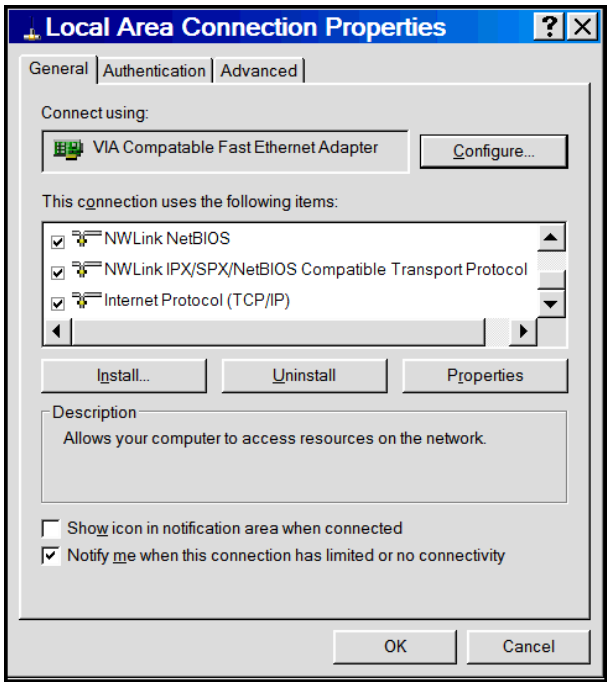
Set Your PC's TCP/IP Address for Ethernet Functionality

The following directions establish a TCP/IP connection at the pc so the PC can communicate with the router. The following directions were written using a Windows XP/ 2003+ operating system.

1. Click Start | Control Panel. Double-click the Network Connections icon.

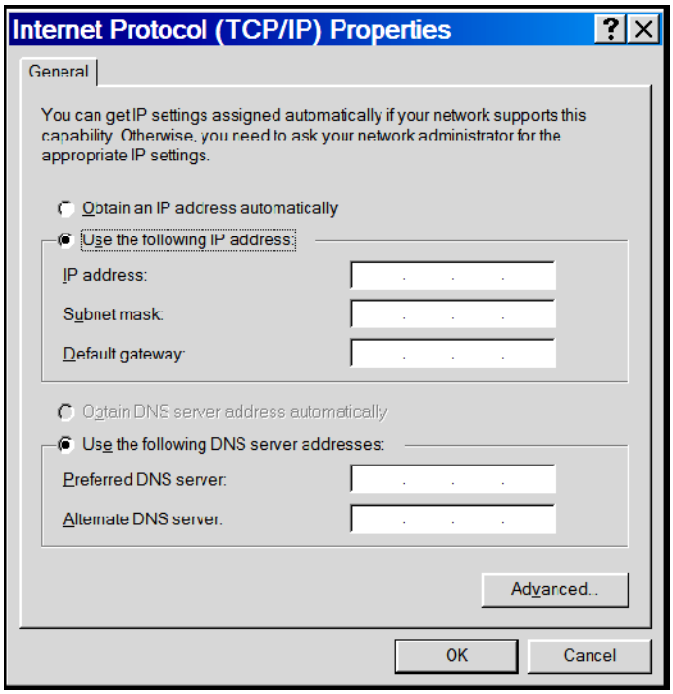


2. The **Network Connections** screen displays. Right-click the **Local Area Connection** icon and choose **Properties** from the drop down list.


Local Area Connection Properties
General Authentication Advanced
Connect using:
VIA Compatable Fast Ethernet Adapter
Configure...
This connection uses the following items:
NWLink NetBIOS
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Allows your computer to access resources on the network.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK Cancel

3. The Local Area Connection Properties dialog box displays.
   - Select Internet Protocol [TCP/IP].
   - Click the Properties button. The Internet Protocol (TCP/IP) Properties screen displays.

4. The Internet Protocol (TCP/IP) Properties screen.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Important Note:

If this screen opens and displays your current IP configuration, we suggest you record this information for future reference (i.e., after the router is configured, you may wish to return this PC to its original settings).

- To set a Fixed IP Address for the pc, select **Use the following IP address**.
  - Enter the pc **IP Address**. Example: 192.168.2.x.

  Note: The **x** in the address stands for numbers 101 and up.

  - Enter the pc **Subnet Mask**. Example: 255.255.255.0
  - Enter the pc **Default Gateway**. Example: 192.168.2.1

    Note: The pc settings must be in the same subnet range as the router.

    The factory default settings for the router are:

    IP Address: 192.168.2.1

    Subnet Mask: 255.255.255.0

    Default Gateway: 192.168.2.2

  - Select **Use the following DNS server addresses**.
    - Enter the IP Address for the **Preferred DNS Server**. Example: 205.171.3.65
    - Click **OK**.
  - Close the **Local Area Properties** screen by clicking **OK**.
  - Close the Control Panel.
  - Repeat these steps for each PC on your network.

AT Command for Verifying Signal Strength

To communicate directly with the cellular modem to verify signal strength, network registration, and roaming status, telnet to the modem.

Note: Ensure that the Status LED is blinking, indicating that the router is ready.

1. To Telnet to the modem. You can access the modem thru the Run icon or from the Command Prompt:

   Click **Start I Run** icon. In the Open window, enter **cmd** and then press **ENTER**.

   or

   Click **Start I All Programs I Accessories I Command Prompt**

   - In the command window, type **telnet 192.168.2.1 5000**
   - At the Login prompt, type the default user name: **admin** (all lower-case). Press **ENTER**
   - At the Password prompt, type the default password: **admin** (all lower-case). Press **ENTER**
2. In the command window, type **AT+CSQ**
3. The router responds with the received signal strength (rssi) and the channel bit error rate (ber).
   RSSI ranges from 0 to 31. BER ranges from 0 to 7 (7 is the highest error rate).

Signal Strength – RSSI	
10 – 31	Sufficient
0 – 9	Weak or Insufficient
99	Insufficient

AT Command for Checking Network Registration and Roaming Status

Use this command to verify that the MultiModem rCell Router has been registered on a wireless network.

1. In the command window, type **AT+CREG?**
2. The router will respond in one of the following ways:

Network Registration Verification	
Value	Network Registration Status
+CREG: 0,0	The router is not registered on any network
+CREG: 0,1	The router is registered on the home network
+CREG: 0,5	The router is registered on a network and it is roaming

Note: If the router indicates that it is not registered, verify the signal strength to determine if the problem is the strength of the received signal.

Exiting Modem Mode

1. After the last AT Command is entered, press:

   CTRL +] (the right bracket).
2. The following prompt displays:

   telnet>

   Type **quit** and press **Enter**.
3. Then the following prompt displays:

   c:>

   Type **exit** and press **Enter**.

Configure the Ethernet Interface Using the Web Management Software

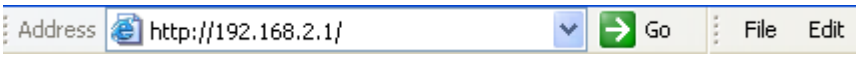
You are now ready to configure the Ethernet interface. This is accomplished by using the router's factory-installed Web Management software. The software is accessed through a Web browser.

1. **Open a Web browser**

   From the pc, open a Web browser.

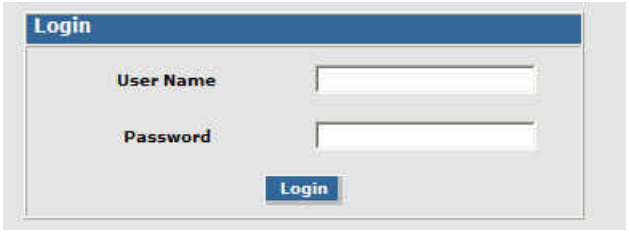
   Note: Ensure that the Status LED is blinking, indicating that the router is ready.

2. Type the default Gateway Address: http://192.168.2.1



3. **Login**

   After entering the Address, the **Login** screen displays.



- Type the default User Name: **admin** (all lower-case).
- Type the default password: **admin** (all lower-case).

  Note: The **User name** and **Password** are case-sensitive (both must be typed in lower-case).

  A password can be up to 12 characters. If Windows displays the **AutoComplete** screen, you may want to click **No** to tell the Windows OS not to remember the password; this helps maintain PC security.

  Password Caution: It is recommended that you change the default password to better protect the security of your router. Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

- Click the **Login** button. The Web Management Home screen displays.

4. **Use the Wizard Setup for Quick Configuration**

   A quick way to configure the router is to use the *Wizard Setup*. The *Wizard Setup* can be opened by clicking the words *Wizard Setup* located under the Web Management software's menu bar. The information entered here will default to other screens that require this information.

   ### Benefits of Using the Wizard Setup

   - Saves time by allowing you to configure the basic setup in one screen.

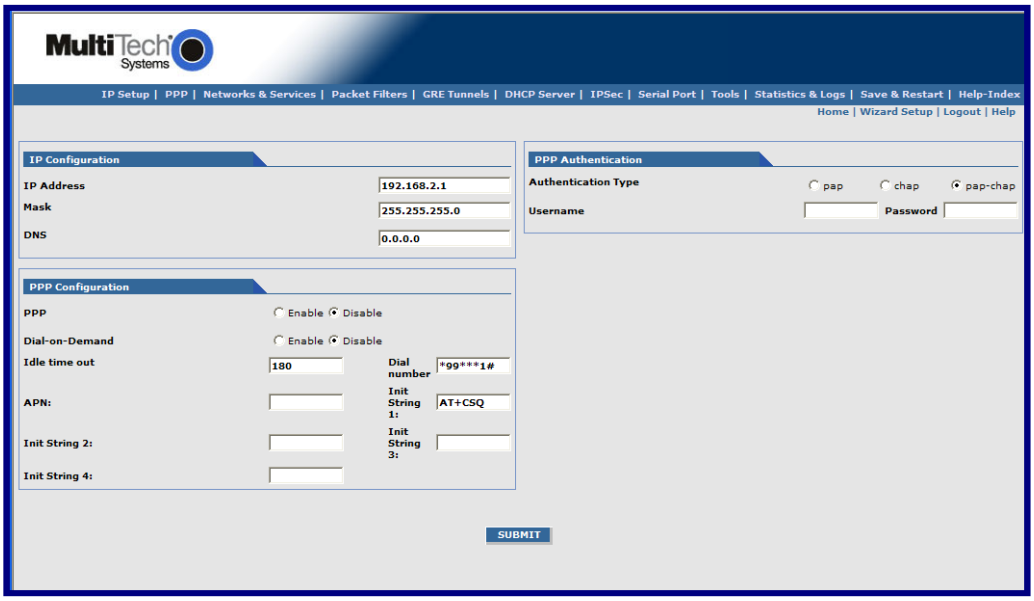
     Note: Additional features and functions can be set up using the complete Web Management software program, described in Chapter 3.

   - Provides a short way to enter and save information needed to create a connection to the Internet.

   Select **Wizard Setup**

MultiTech Systems
IP Setup | PPP | Networks & Services | Packet Filters | GRE Tunnels | DHCP Server | IPSec | Serial Port | Tools | Statistics & Logs | Save & Restart | Help-Index
Home | Wizard Setup | Logout | Help

5. After clicking the **Wizard Setup** selection, the *Wizard Setup* screen displays.



Wizard Setup

A minimum router configuration is provided using the Wizard Setup. This provides a quick way to enter and save information needed to create a connection to the Internet. The table below provides the information for the minimum configuration.

IP Configuration	
IP Address	The default is 192.168.2.1. To change it, simply enter your own IP address.
Mask	The default is 255.255.255.0
DNS	Enter the primary DNS IP address for the system. The default is 0.0.0.0

PPP Configuration	
PPP	The default is ***disable***. To connect to the Internet, you need to enable PPP. Depending on the model, commands may need to be issued to the integrated cellular modem before connecting to the wireless service. To issue commands to the integrated cellular modem, PPP must be disabled and telnet port 5000 used.
Dial-on-Demand	The default is ***disable***.
Idle Time Out	Sets the amount of time the PPP link stays active before disconnecting. Setting the value to zero causes the link to stay active continuously.
Dial Number	Enter the dial number. This number connects you to the Internet. For HSDPA, the number is *99***1#.
APN	For HSDPA, enter the APN (Access Point Name). The APN is assigned by your wireless service provider.
Init String	You can set up to 4 router initialization strings.

PPP Authentication	
Authentication Type	Click the button corresponding to the authentication protocol you want to use to negotiate with the remote peer. PAP, CHAP, or PAP-CHAP. Default = PAP-CHAP
Username	Enter the PPP Username. This name authenticates the remote peer.
Password	Enter the PPP Password. This password authenticates the remote peer.

A Note About the Access Point Name

The APN (Access Point Name) is assigned by your HSDPA wireless service provider, but you may have to ask for it. An access point is an IP network to which a MultiModem rCell Router connects. The Web Management software asks for the APN on the *Wizard Setup* screen and the *PPP* screen.

Important Note About Provider Fees

Your provider will charge you for your data usage. Please check with your provider to make sure you are aware of the charges.

If you plan to use the router for large amounts of data transfers, Multi-Tech recommends an unlimited data plan with your account. Multi-Tech will not be responsible for any charges relating to your cellular bill.

Note: Additional features and functions can be set up using the complete Web Management software program, described in Chapter 3.

6. Click the **Submit** button.
7. Click the Save & Restart button (located on the Menu bar). The router will reboot

IMPORTANT NOTE ABOUT *SUBMIT* AND *SAVE & RESTART*

> Click the **Submit** button located at the bottom of most screens in order to save any changes you make. Then you click the **Save & Restart** button, located on the Menu bar, in order for your settings to take effect. **Save & Restart** does not have to be executed after each screen; you can change and Submit several screens, and then click **Save & Restart**.

8. The Status LED will go out during a 'Save & Restart'. Once it is flashing, the unit is ready to go.
9. Open a Web browser, assume that all configurations are correct and the router's CD LED is ON, you should now be able to browse the internet.

Shutdown Caution

> Never unplug the power until you have first performed the **Save & Restart** process. If the setup changes are not properly saved before unplugging the power, data could be lost.

Chapter 3 – Using the Web Management Software

The Web Management software configures the Ethernet functionality of your router.

Navigating the Web Management Software

This section explains the menu structure and the navigation buttons of the router's Web Management software.

Menu Bar
MultiTech Systems
IP Setup | PPP | Networks & Services | Packet Filters | GRE Tunnels | DHCP Server | IPSec | Serial Port | Tools | Statistics & Logs | Save & Restart | Help-Index
Home | Wizard Setup | Logout | Help

IP Setup: Sets up a General Configuration, HTTP, DDNS, SNTP, Static Routes, and Remote Configuration.

PPP: Sets up the PPP authentication, dial-on-demand, router authentication, and Wakeup on Call.

Networks & Services: Defines networks and services to make them available to other functions such as allowed packet filters, static routes, remote configuration, DNAT, and GRE tunnels and routes.

Packet Filters: Defines filter rules, DNAT configuration, and ICMP rules.

GRE Tunnels: Generic Routing Encapsulation (GRE). Defines the remote network and the tunnel through which traffic is to be routed.

DHCP Server: Configures the DHCP server settings.

IPSec: Allows device to support LAN-to-LAN VPN tunneling with DES,3DES and AES encryption support

Serial Port: Adds support for RS-232 serial port so that Ethernet and legacy serial devices can share the same cellular connection.

Tools: Sets DDNS Force Update and Reset router, displays Service Status, and provides screens for

Firmware Upgrade, Load Configuration, and Save Configuration.

Statistics & Logs: Shows statistics and logs maintained by the router.

Save & Restart: Saves your settings and reboots your router.

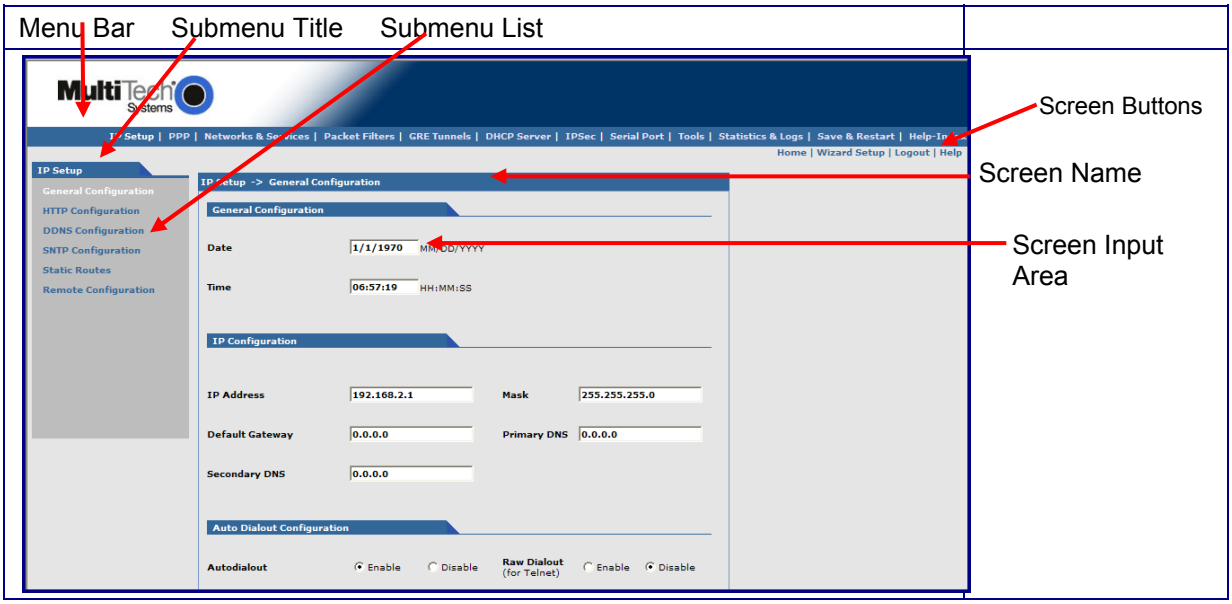
Help Index: Accesses the online Help text.

IMPORTANT NOTE ABOUT *SUBMIT* AND *SAVE & RESTART*

Click the **Submit** button located at the bottom of most screens in order to save any changes you make.

Then you must click the **Save & Restart** button, located on the Menu bar, in order for your settings to take effect. **Save & Restart** does not have to be executed after each screen; you can change and **Submit** several screens, and then click **Save & Restart**.

Screen Parts



Screen Buttons

Home: Click this button to return to the Home screen.

Wizard Setup: Click this button to display the Wizard Setup screen on which you can quickly set up your MultiModem rCell Router with basic configuration settings.

Logout: Click this button to Logout and return to the login screen.

Help: Click this button to display the Help text.

Submenus

The submenus display on the left side of the screen.

The following table shows the sub-menu selections under each main menu category.

IP Setup	PPP	Networks & Services	Packet Filters	GRE Tunnels
General Configuration HTTP Configuration DDNS Configuration SNTP Configuration Static Routes Remote Configuration	PPP Configuration Wakeup on Call Power On Config Modem Commands	Network Configuration Service Configuration	Packet Filters DNAT Configuration Advanced	GRE Tunnels GRE Routes
DHCP Server	**IPSec**	**Serial Port**	**Tools**	**Statistics & Logs**
Subnet Settings Fixed Addresses	Add IKE Connection Add Manual Connection	Serial Port Settings Serial Port Configuration Client Settings TCP/UDP-Client Configuration Server Settings TCP/UDP-Server Configuration	Tools Firmware Upgrade Load Configuration Save Configuration	Ethernet PPP PPP Trace SysInfo DHCP Statistics GRE Statistics Modem Info Service Status TCP/UDP Client Live Log TCP/UDP Server Live Log IPSec Live Log IPSec Log Traces

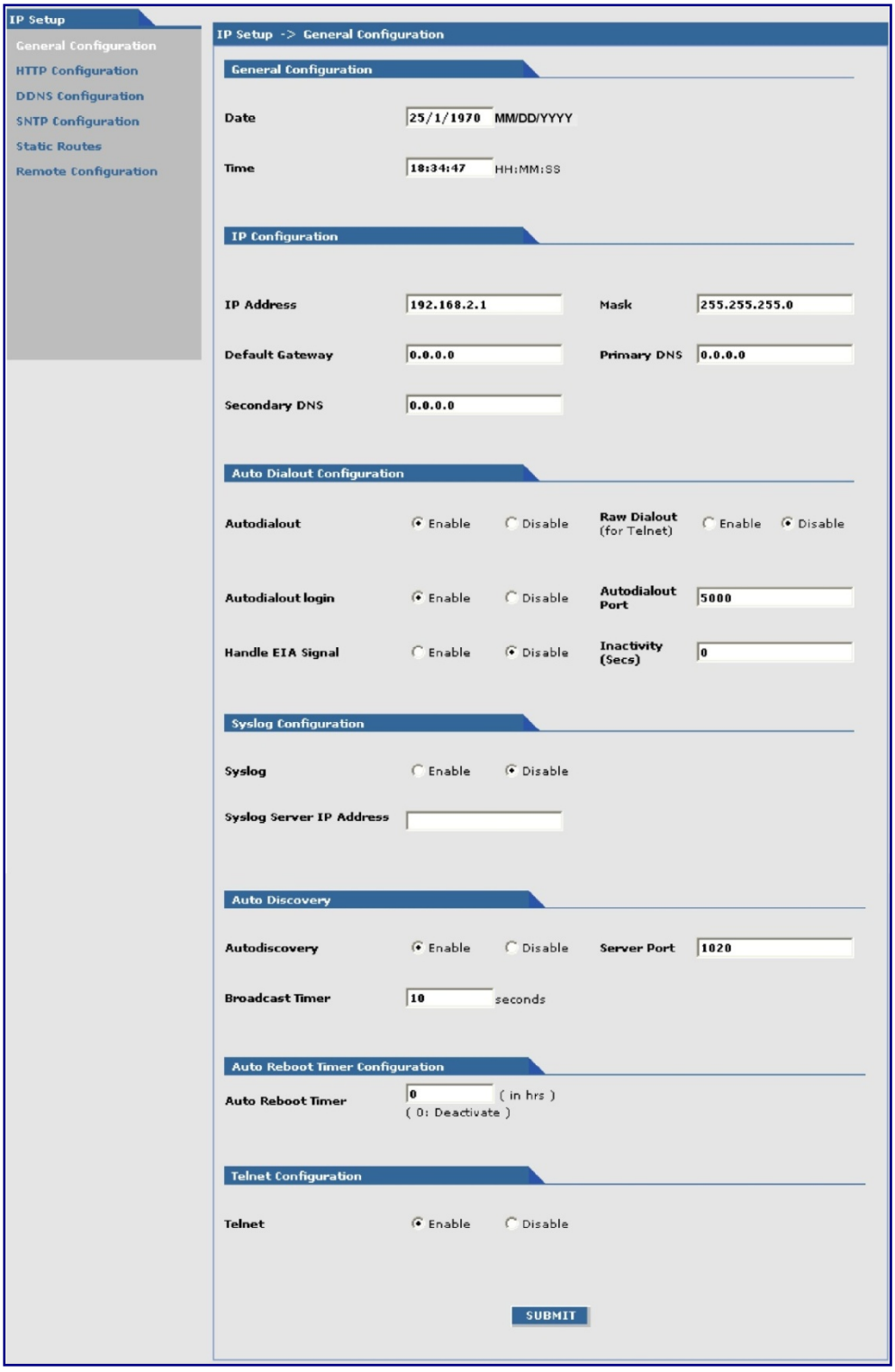
Web Management Software Screens

The rest of this chapter describes each of the Web Management software screens.

IP Setup

IP Setup › General Configuration

In the General Configuration, you will set the general system-based parameters.



General Configuration

Date and Time: The system date and time display in these formats: **MM/DD/YYYY** / **HH:MM:SS**. A real time clock is part of SNTP to display proper time.

IP Configuration

Enter the following addresses for the Ethernet interface.

IP Address (Default = 192.168.2.1), Mask (Default 255.255.255.0), Default Gateway (Default 0.0.0.0),

Primary DNS (Default 0.0.0.0), Secondary DNS (Default 0.0.0.0).

Note: See Appendix A – Table of Commonly Supported Subnets.

Auto Dial out Configuration

Auto Dialout: Check the box to enable/disable Auto Dialout. Default = Enable. The Auto Dialout settings allow you to use the integrated cellular modem directly with no router functionality. This is accomplished using redirector software on your pc. This software creates a virtual serial port allowing your pc to communicate with the integrated cellular modem over IP using telnet.

Raw Dialout: Check the box to enable/disable raw mode for an Auto Dialout session. Default = Disable.

Auto Dialout Login: Check the box to enable or disable Auto Dialout Login feature. Default = Enable. The Auto Dialout port is the telnet port used by the redirector software on your pc to communicate to the integrated cellular modem.

Auto Dialout Port: Enter the serial Auto Dialout Port number. Default = 5000.

Handle EIA Signal: Check the box to enable/disable the EIA standard signal characteristics (time and duration) used between different electronic devices.

Inactivity: Enter the time in seconds that the auto dialout session will stay active before going inactive.

Syslog Configuration

Syslog: Check the box to enable or disable Syslog. Default = Disable.

Syslog Server IP Address: If a Remote Syslog Server IP Address is specified, the syslog feature acts as a remote Syslog.

Auto Discovery

Auto Discovery: Check the box to enable or disable Auto Discovery to broadcast (MAC level), the MAC Address, IP Address, and DHCP information to the configured server port. Default = Enable. The router will send a broadcast packet on the specified server port every 10 seconds or whatever interval the broadcast timer is set to.

Server Port: Enter the Server Port Number. Default port is 1020.

Broadcast Timer: Enter the amount of time in seconds for the auto-discovery packet granularity of periodic broadcasting. Default is 10 seconds.

Auto Reboot Timer Configuration

Auto Reboot Timer: Enter the number of hours to lapse between each automatic reboot. The default of zero deactivates the timer. Range is 0 to 999.

Telnet Configuration

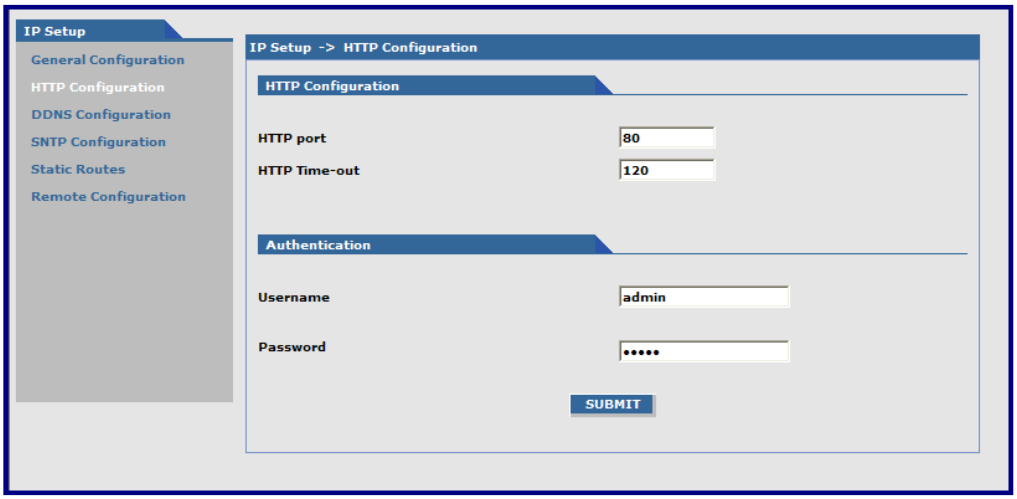
Enables/Disables the Telnet port. The default is **Enable**. This is specifically for telnet port 23 for technical support debug. You can still access the integrated cellular modem using port 5000 when this is disabled.

Submit Button

Click the **Submit** button to save these settings.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup › HTTP Configuration



HTTP Configuration

HTTP Port: Enter the port number on which the HTTP server will listen for requests. Default is 80.

HTTP Time-0ut: Set the HTTP session in seconds. The default is 120 seconds.

Authentication

Username: Enter the Username that can access to the Web Management software. Default is **admin**. This username and password are also used for telnet access to the router and integrated cellular modem.

Password: Enter the Password for access to the Web Management software. Default is **admin**.

Note: You should change the password to one of your choosing. It can be up to100 characters. Use a safe password. Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

Submit Button

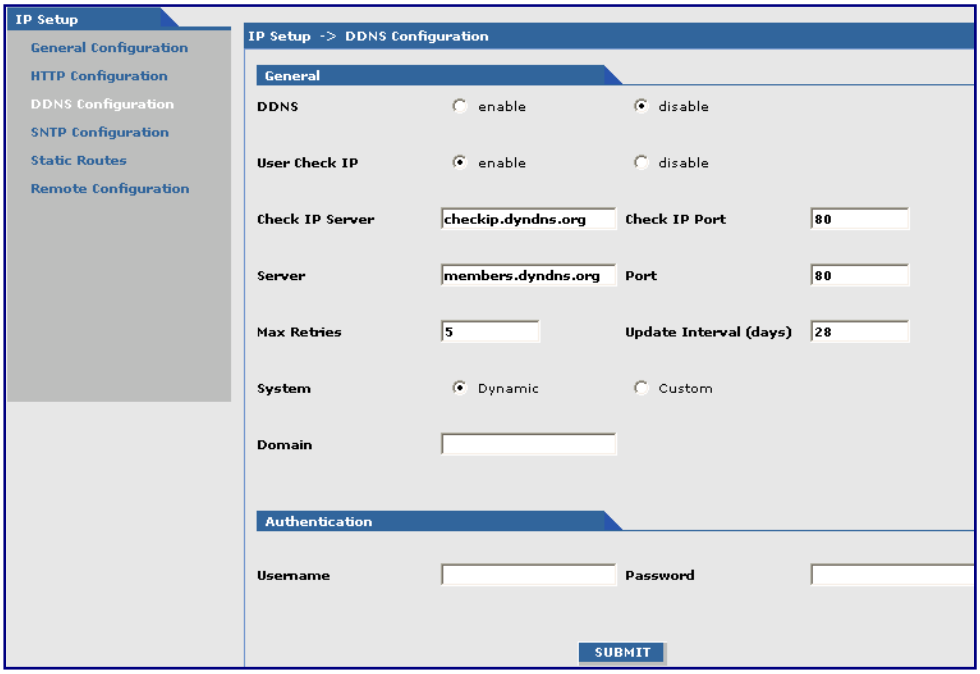
Click the **Submit** button to save these settings.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup › DDNS Configuration

DDNS (Dynamic Domain Naming System) allows you to have a static domain name with a dynamic IP address. Whenever your dynamic IP address changes, it is submitted to the DDNS server where your domain name is updated to point to the new IP address.

Note: You have to register with a DDNS server to use this feature.



General

DDNS: Check the Enable or Disable box. This enables/disables DDNS. Default = Disable.

Use Check IP: Check the Enable or Disable box. If enabled, the program will query the server to determine the IP address before it performs the DDNS update (the IP address is still assigned by the wireless provider and the DDNS will be updated based on the address returned by Check IP Server). If disabled, the program will perform the DDNS update using the IP address that it obtains from the PPP link. Default = Enable.

Check IP Server: Enter the Server name from which the currently assigned IP address is obtained. This check IP server is a server the router accesses to check it's current IP address.

Check IP Port: Enter the port number of the *Check IP Server*. Default is 80.

Server: Enter the Server name to which the IP Address change is registered. Example: *members.dyndns.org*

Port: Enter the Server port number. Default is 80.

Max Retries: Enter the maximum number of tries that will be allowed if the update fails. Default = 5. Range is 0 – 100.

Update Interval: Enter the intervals in days that will be allowed to pass when there is no IP Address change. At the end of this interval, the existing IP Address will be updated in the server so that it will not expire. Default = 28 days. Range is 1 – 99 days.

System: Sets the system registration type as either Dynamic or Custom. Default = Dynamic.

Domain: Enter the registered Domain name.

Authentication

Username: Enter the Username that can access the DDNS Server. Default = NULL. You should have received your username when you registered with the DDNS service.

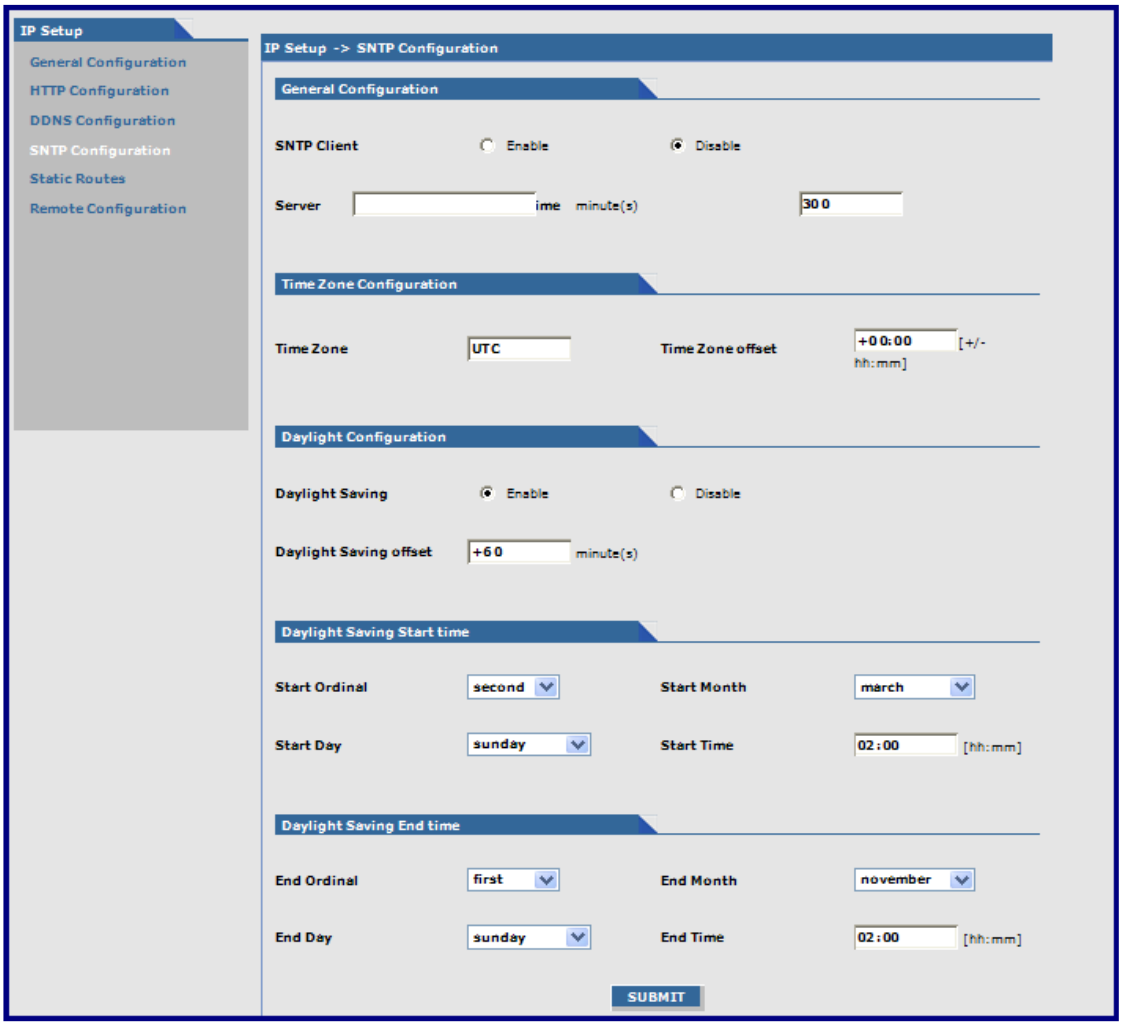
Password: Enter the Password that can access the DDNS Server. Default = NULL. You should have received your password when you registered with the DDNS service.

Submit

Click the **Submit** button to save these settings.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup › SNTP Configuration



General Configuration

SNTP Client: Enable or disable the SNTP Client to contact the configured server on the UDP port 123 and set the local time. The default is *Disable*.

Server: Enter the SNTP server name or IP address to which the SNTP Client must contact in order to update the time. No default.

Polling Time: Enter the polling time at which the SNTP client requests the server to update the time. Default is 300 minutes. Time must be entered in minutes.

Time Zone Configuration

Time Zone: Enter your time zone. Default = UTC (Universal Coordination).
See the following Web site for Time Zone information: http://wwp.greenwichmeantime.com/info/timezone.htm

Time Zone Offset: Enter +/- hh:mm. Default = +00:00. Offset is the amount of time varying from the standard time of a Time Zone.

Daylight Configuration

Daylight Saving: Enables/disables Daylight Saving mode. The default is *Enable*.

Daylight Saving Offset: Set the offset to use during Daylight Saving mode. Default is +60 minutes. Enter the time in + / - minutes.

Daylight Saving Start Time

Start Ordinal: Set the start ordinal to use during Daylight Saving mode. Options are first/second/third/fourth/last. Default is first. Daylight Saving time usually starts at the same time on the same day of the week in the same month every year. Each day of the week occurs four or five times a month. Therefore, you will be selecting the week in which daylight saving time starts: the first, second, third, fourth or the last of the month.

Start Month: Set the start month to use during Daylight Saving mode. Default is April.

Start Day: Set the start weekday to use during Daylight Saving mode. Default is Sunday.

Start Time: Set the start time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Daylight Saving End Time

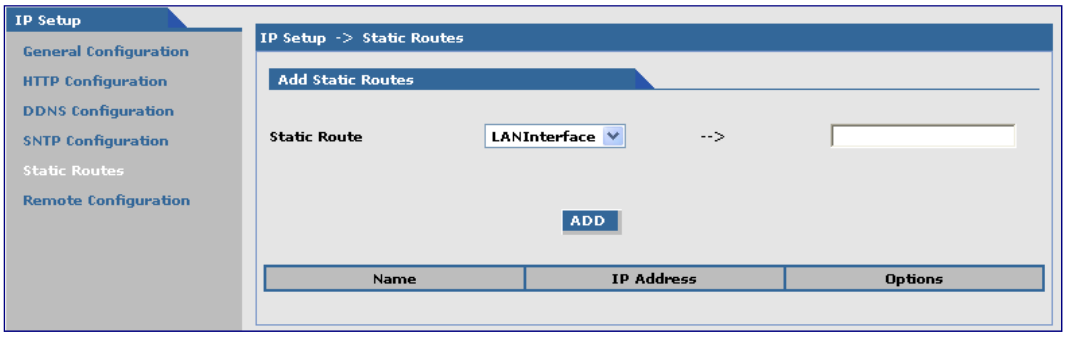
End Ordinal: Set the end ordinal to use during Daylight Saving mode. Select the week in which daylight saving time ends. Options are first/second/third/fourth/last. Default is last.
End Month: Set the end month to use during Daylight Saving mode. Default is October.
End Day: Set the end weekday to use during Daylight Saving mode. Default is Sunday.
End Time: Set the end time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Submit Button

Click the **Submit** button to save these settings.
Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup › Static Routes

Routing information is used by every computer connected to a network to identify whether it is sending a data packet directly to the firewall or passing it on to another network. The options to Delete or Edit a route after it has been defined and added are available by using the table at the bottom of the screen.

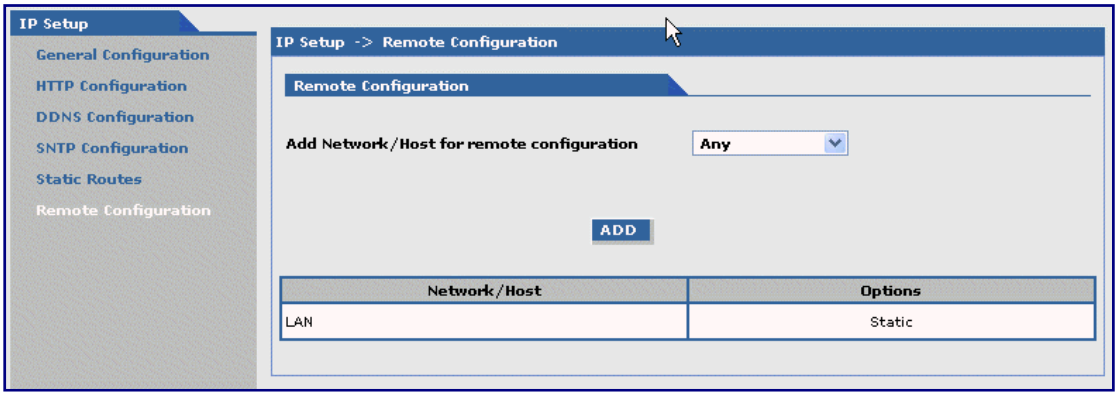


Add Static Routes

IP packets destined for the network indicated in the drop down box are routed to the IP address in the box pointed to by the arrow. The networks in the drop down box can be defined under the 'Networks & Services' tab.

Static Route: Select a static route from the drop down list box, and then click the **Add** button.
Add Button: After clicking the **Add** button, the new route is added and will display at the bottom of the screen.
Important Note: The Static Route screen will not display until the network is defined under **Networks & Services.**

IP Setup › Remote Configuration



Remote Configuration

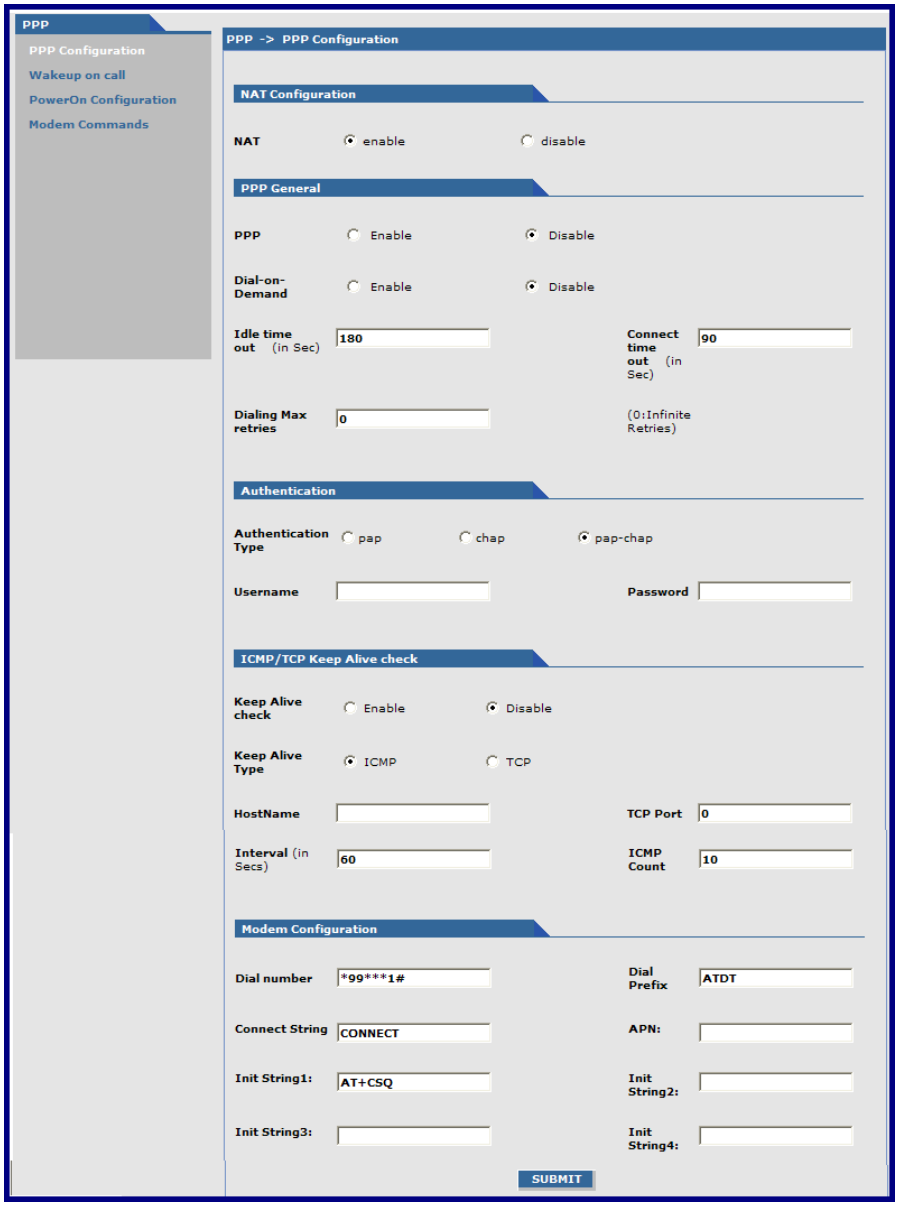
Add Network/Host for Remote Configuration:

Select a network or host from the drop down box. You can define more network or host under the **Network & Services** tab. The choices are Any, LAN, and WAN Interface. Choose all that apply. Click the **Add** button after each selection.

Add Button: After clicking the **Add** button, the network or host is added and displays at the bottom of the screen.
Delete: You will have the option to delete **Any** and **WAN Interface** in the **Options** window once it is added. Click on Delete in the Options window.

PPP

PPP › PPP Configuration



NAT Configuration

NAT Enable/disable NAT (Network Address Translation). The default is *Enable*.

If NAT is enabled:

- Your LAN can use one set of IP addresses for internal traffic and a second set of addresses for external traffic. In other words, the router with NAT does the simple IP routing between the LAN interface and the WAN interface. NAT hides the LAN address behind a single IP address on the wireless side.
- Your internal addresses are shielded from the public Internet.

If NAT is disabled:

- The router functions without performing any address translation on the packets passing through it.
- Masquerading of packets originating from the LAN is disabled.
- Address translation of packets arriving from the WAN is also disabled.
- Any DNAT Configuration previously setup in the DNAT Configuration screen is disabled. This prevents the user from adding any DNAT rules, which if allowed would defeat the purpose of enabling Routing.

Note: For routing to take effect, the configuration must be saved after enabling it. It won't be effective on the fly at runtime.

PPP General

PPP Enable/disable PPP. The default is *Disable*. When enabled, the unit functions as a router. PPP must be disabled to access the integrated cellular modem directly using telnet port 5000. If PPP is enabled, you cannot access the integrated cellular modem.

Dial-on-Demand: Enable/disable Dial-on-Demand. The default is *Disable*. If you disable it, the router will always stay connected unless the Idle Time Out expires. When Dial-on-Demand is enabled, use the 'Wakeup on Call' settings under the PPP menu to configure the settings for re-establishment of the connection.

Idle Time Out: Set the amount of idle time that will pass before the router will timeout. The default is 180 seconds. If the time expires, the PPP connection to the Internet will disconnect. Any IP packets from the LAN side or IP traffic from the wireless side will reset this timer and prevent the connection from dropping.

Connect Time Out: Set the number of seconds to wait for a connection while in receive mode before timing out.

Dialing Max Retries: Enter the number of dialing retries allowed. The default is zero, which means an infinite number is allowed. Range 0 to 100.

Authentication

Authentication Type: Set the authentication protocol type that will negotiate with the remote peer: pap/chap/pap-chap. Default is pap-chap.

Username: Enter the Username with which the remote peer will authenticate. You can leave this field blank, if desired. Username is limited to 60 characters.

Password: Enter the Password with which the remote peer will authenticate. You can leave this field blank, if desired. Password is limited to 60 characters.

ICMP Keep Alive Check

Keep Alive Check: Enable/disable Keep Alive Check. The default is *Disable*. This is used to periodically check that the Internet connection is up. If it is not, the router will try to reconnect.

Keep Alive Type: Select ICMP or TCP (the protocol type for Keep Alive).

Host Name: Enter the Host Name or IP Address for Keep Alive Check. No default.

TCP Port: Enter the TCP Port number to connect with the TCP server.

Interval: Set the number of seconds for Keep Alive Check. Default is 60 seconds.

ICMP Count: Set the number of ICMP Keep Alive Checks to be sent to the specified host. Default is 10.

Modem Configuration

(Refer to the Customer Activation Notices included with the product for proper information to enter).

Dial Number: Set the dial number to be dialed. Default is NULL. The dial number is ***99***1#**.

Dial Prefix: Set the modem dial prefix. The default is ATDT.

Connect String: Set the modem Connect String. The default is CONNECT.

APN: Enter the APN (Access Point Name). The APN is assigned by your wireless service provider.

Init String 1-4: Configure the modem init strings. You can set up to 4 modem initialization strings.

Submit Button

Click the **Submit** button to save these settings.

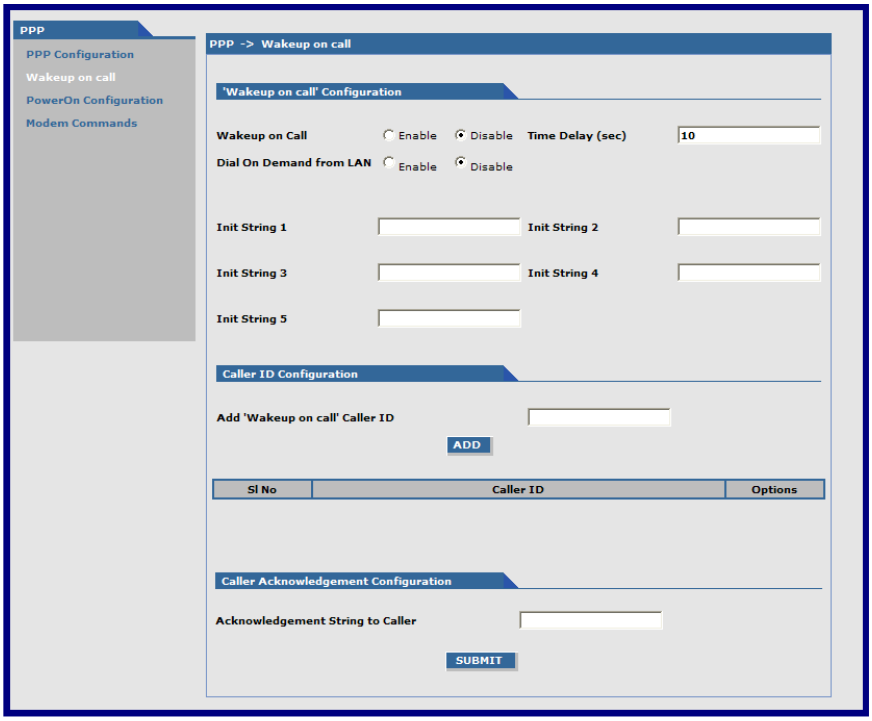
Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

Note: The MTCBA-H-EN2 is shipped with command AT^SLED=1 entered at Init String 2. If the MTCBA-H-EN2 is set back to factory default using the pushbutton on the back of the chassis, this command will need to be reentered and saved as Init String 2 for the LS LED to display properly.

PPP > Wakeup-on-Call

The Wakeup-on-Call feature allows the router to wake up and initiate a connection when there is an incoming call or LAN activity. If you desired some security with this feature, you can set up the router to wake up based on Caller ID or SMS instead of allowing all incoming calls to wakeup the router. Dial-on-Demand in the IP Setup menu must be enabled for these settings to have any affect. The Wakeup-on-Call feature will reduce the cost incurred when a router is online and available 24/7.

Note: When provisioning this feature, you must allow incoming calls, sms capability, and/or caller-id.



Wakeup-on-Call Configuration

Wakeup on Call: Enable/disable the Wakeup-on-Call feature. The default is *Disable*. Wakeup on Call occurs when a ring or caller ID is detected. This will trigger the router to reconnect after the 'Time Delay' expires.

Time Delay: Enter the amount of time that you want to pass between the reception of a call and the initiation of the Wakeup-on-Call connection. A time delay is needed to make sure that the incoming call has ended before the connection is initiated. The default is 10 seconds.

Dial-on-Demand from LAN: The default is *disable*. When enabled, the router will reconnect when it sees IP traffic on the LAN is needed to route. If this feature is disabled, Dial-on-Demand initiates a PPP connection to the Internet only from the WAN, not from the LAN.

Init Strings: Configure the router initialization strings. These init strings need to be specific to the integrated cellular modem. Some initialization may be required for the integrated cellular modem to accept SMS for 'Wakeup on Call'. Init-num can range from 1-5. The default is NULL. Refer to the following examples.

Submit: Click the **SUBMIT** button to save these settings.

Caller ID Configuration

Add "Wakeup on Call" Caller ID: To add *Caller ID* to the *Wakeup-on-Call* function, enter the *Caller ID* to be allowed to wakeup the router. Enter 'Ring' to wake up on any call. Enter a CID phone number or an SMS message. The SMS message string must not contain any spaces between words.
After entering the *Caller ID*, click the **Add** button. The *Caller ID* displays at the bottom of screen. You can enter any number of IDs you desire.
A Caller ID can be edited or deleted using *Options*, which will be available once a Caller ID is displayed.

Caller Acknowledgement Configuration

Acknowledgement String to Caller: The configured string of (0 to 40 characters) will be sent to the integrated cellular modem upon receiving a valid caller ID from the WAN. The default is NULL string.
Note: If the string is not configured, acknowledgement to the caller will not be sent upon successful caller ID reception.

Submit

Click the **SUBMIT** button to save these settings.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

PPP > Wakeup-On-Call Examples

Example 1 – Set Up the Ethernet Router to Activate on Incoming SMS Message

1. On the ***PPP > PPP Configuration*** screen, set up the following parameters:

   PPP General
   - Make sure that **PPP** is *Disabled* (the default).
   - Make sure **Dial-on-Demand** is *Disabled* (the default).
   - Set the **Idle Time Out** to the number of seconds you desire.

   Authentication
   - Your wireless service provider may require you to have a separate PPP *Username* and *Password*. If so, enter them here. **Note:** If a username and password are required, your wireless provider would have given them to you when you activated your account.

   Modem Configuration
   - Make sure your **Dial Number** is entered correctly: The Dial Number is ***99***1#**
   - Enter your **APN.** The APN is assigned by your wireless service provider.
     Example: AT+CGDCONT=1,"IP","Internet" The Example: AT+CGDCONT=1,"IP","Internet" needs to be removed. Just the APN name needs to be entered in the APN field.

   Submit
   - Click the **Submit** button to save the changes made on this screen.
2. On the ***PPP > Wakeup-on-Call*** screen, set up the following parameters:

   Wakeup-on-Call Configuration
   - Select *Enable* for **Wakeup-on-Call**.
   - Set the **Time Delay**. You can use the 10 second default.
   - Enter the Init Strings so that the integrated cellular modem receives SMS.
     Enter Wakeup Init String 1 as at+cmgf=1
     Enter Wakeup Init String 2 as at+csms=1
     Enter Wakeup Init String 3 as at+cnmi=2,2,0,0,1
     Enter Wakeup Init String 4 as at^scfg="URC/DstIfc",mdm
   - Click the **Submit** button to save these settings.

   Caller ID Configuration
   - Enter an SMS that you want added to the Caller ID list.
     Note: Add the SMS message string into the Caller ID list. The SMS message string must not contain any spaces between words. When the configured string matches the SMS message string, it will activate the Wakeup-on-Call feature.
   - **Add** Button
     Click the **Add** button to save each message as it is entered into the Caller ID list.

   Caller Acknowledgement Configuration
   - Enter a configured string (0 to 40 characters) that will be sent to the integrated cellular modem upon receiving a valid Caller ID from the WAN.
     Set the Wakeup Acknowledgement string configuration with the command **at+cnma**
   - Click the **Submit** button to save the Acknowledgement Configuration.

   You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Example 2 – Determine if the router Is Supporting Incoming Calls and Caller ID

1. On the ***PPP > PPP Configuration*** screen, make sure that **PPP** is ***Disabled***.
2. On the **PPP > Wakeup-on-Call** screen, make sure that **Wakeup-on-Call** is ***Disabled***.
3. Open a command prompt by clicking the **Start** button and selecting **Run**.
4. Type **CMD** to open the command window. Click **OK**.
5. When the command window opens, type **Telnet 192.168.2.1 5000.** This is the IP address of the router.
   Note: 5000 is the port number.
   - **5.1.** Enter your username and password to login.
   - **5.2.**Enter an AT command to make sure you receive a response; i.e., *OK*.
   - **5.3.**Enter the Command **AT+CNUM** to determine the dial number of your router.
6. From another phone, call your router using the number identified in Step 5.3. This will let you know if the RING message shows.
7. To enable Caller ID, enter the **AT+CLIP=1** command on the command screen and make the call again to see if it shows Caller ID information.

   Notes:
   - Step 5.3 must show the RING or CALLER ID information in order for the Wakeup-on-Call function to work.
   - Some wireless providers might not provide caller ID information if you have only a data plan.

Example 3 – Set Up the Ethernet Router to Activate on ALL Incoming Calls

1. On the ***PPP >PPP Configuration*** screen, set up the following parameters:

PPP General

- Make sure that **PPP** is *Enabled*.
- Make sure **Dial-on-Demand** is *Enabled*.
- Set the **Idle Time Out** to the number of seconds you desire.

Authentication

- Your wireless service provider may require you to have a separate PPP *Use name* and *Password*. If so, enter them here.

Note: If a username and password are required, your wireless provider would have given them to you when you activated your account.

Modem Configuration

- Make sure your **Dial Number** is entered correctly: The Dial Number is ***99***1#**

Submit

- Click the **Submit** button to save the changes made on this screen.

2. On the ***PPP > Wakeup-on-Call*** screen, set up the following parameters:

Wakeup-on-Call Configuration

- Select *Enable* for **Wakeup-on-Call**.
- Set the **Time Delay** to *3* seconds. You can use the 10 second default.
- All **Init Strings** should be empty.
- **Submit** Button
  Click the **Submit** button to save these settings.

Caller ID Configuration

- Enter the string **RING** to the Caller ID list.
- Click the **Add** Button to save the string to the Caller ID list.

3. **Save and Restart**

Click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Example 4 – Set Up the Ethernet Router to Activate on Matching Caller IDs Only:

1. On the ***PPP > PPP Configuration*** screen, set up the following parameters:

PPP General

- Make sure that **PPP** is *Enabled*.
- Make sure **Dial-on-Demand** is *Enabled*.
- Set the **Idle Time Out** to the number of seconds you desire.

Authentication

- Your wireless service provider may require you to have a separate PPP *username* and *password*. If so, enter them here.

Note: If a username and password are required, your wireless provider would have given them to you when you activated your account.

Modem Configuration

- Make sure your **Dial Number** is entered correctly: The Dial Number is ***99***1#**

Submit

- Click the **Submit** button to save the changes made on this screen.

2. On the ***PPP > Wakeup-on-Call*** screen, set up the following parameters:

Wakeup-on-Call Configuration

- Select *Enable* for **Wakeup-on-Call**.
- Set the **Time Delay**. You can use the 10 second default.
- Enter the **Init Strings:**
  Set Wakeup **Init String 1** by entering **AT+CLIP=1**
- **Submit** Button
  Click the **Submit** button to save these settings.

Caller ID Configuration

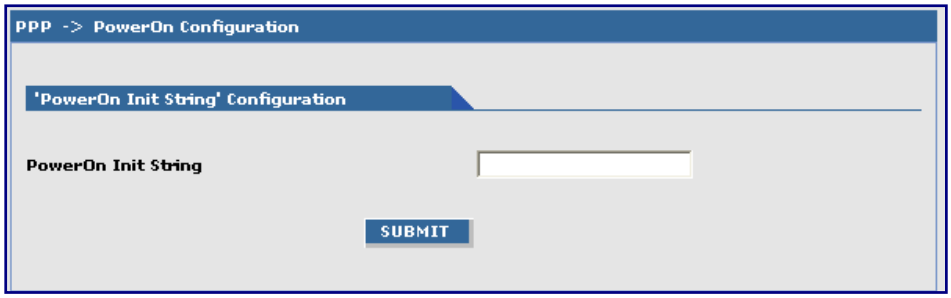
- Enter a caller's ID that you want added to the Caller ID list.
- **Add** Button
  Click the **Add** button to save each Caller ID as it is entered to the Caller ID list.

3. **Save and Restart**

Click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

PPP › Power-On Configuration

The Power-On Configuration feature allows you to set an initialization string that will be sent to the router upon boot up.



Power-On Init String Configuration

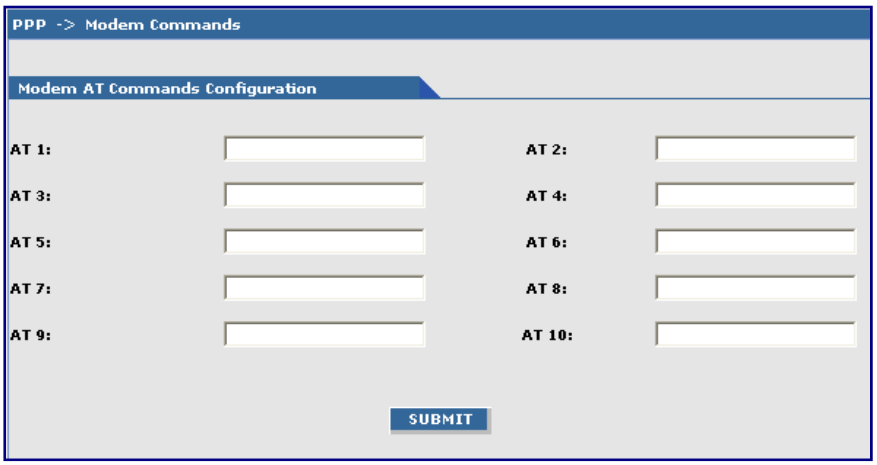
Power-On Init String: You can enter a string of 0 to 40 characters that will be sent to the router upon boot up. All commands will initialize before you proceed with regular PPP related activity.
Note: When no initialization string is configured, regular functionality of the router is retained.

Submit: Click the **SUBMIT** button to save this setting.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

PPP › Modem Commands

Setting up certain modem commands will allow an external application to query modem information (based on the commands entered). The application can use the URL HTTP://192.168.2.1/modeminfor.html to get the IP address that is currently assigned to the integrated cellular modem after the PPP connection is established. It also will show the results of up to ten AT commands entered here.



Modem AT Commands Configuration

These commands will be sent every time a PPP connection to the network is initiated.

Example of Useful HSDPA AT Commands:

AT+CGSN	Product Serial Number
AT+CGMR	Software Version
AT+CNUM	Wireless Subscriber Number
AT+COPS?	Network Information (Operator)
AT+CREG?	Network Registration
AT+CSQ	Signal Quality

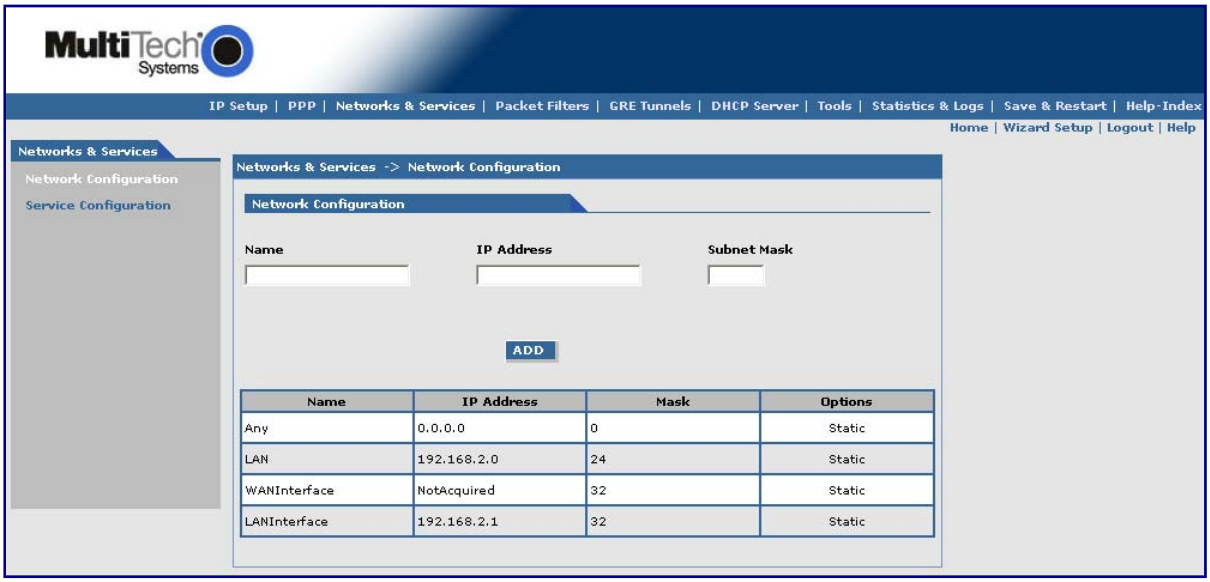
Notes:

- You can also retrieve the integrated cellular modem information without using a browser:
  Make a TCP connection to port 80 (same as the Web Admin port) and send data as:
  GET /atinfor.html HTTP/1.1
  Then press **Enter** twice.
- See the HSDPA AT Command Reference Guide (Number S000453x) for other commands.

Networks & Services

Networks & Services › Network Configuration

Networks or Hosts can be added here. The options to Delete or Edit a network after it has been defined and added are available by using the table at the bottom of the screen.


IP Setup | PPP | Networks & Services | Packet Filters | GRE Tunnels | DHCP Server | Tools | Statistics & Logs | Save & Restart | Help-Index
Home | Wizard Setup | Logout | Help
Networks & Services
Network Configuration
Service Configuration
Networks & Services -> Network Configuration
Network Configuration
Name
IP Address
Subnet Mask
ADD
Name | IP Address | Mask | Options
Any | 0.0.0.0 | 0 | Static
LAN | 192.168.2.0 | 24 | Static
WANInterface | NotAcquired | 32 | Static
LANInterface | 192.168.2.1 | 32 | Static

Network Configuration

Enter the Name, IP Address, and Mask for a new Network or Host.

Notes:

- A Network/Host Name cannot be edited.
- A Network/Host cannot be deleted if it is used in another configuration.
- Network/Host changes are reflected in all the configurations in the Web Management software where they are used.
- A Network/Host added here will be displayed in the following sections: Static Routes, DNAT, and Packet Filters.

Name: Enter the name of the Network/Host. The same address-mask pair should not already be present in the displayed list. The Name is limited to 15 characters maximum.

IP Address: Enter the IP Address of the Network/Host. The same address-mask pair should not already be present in the displayed list.

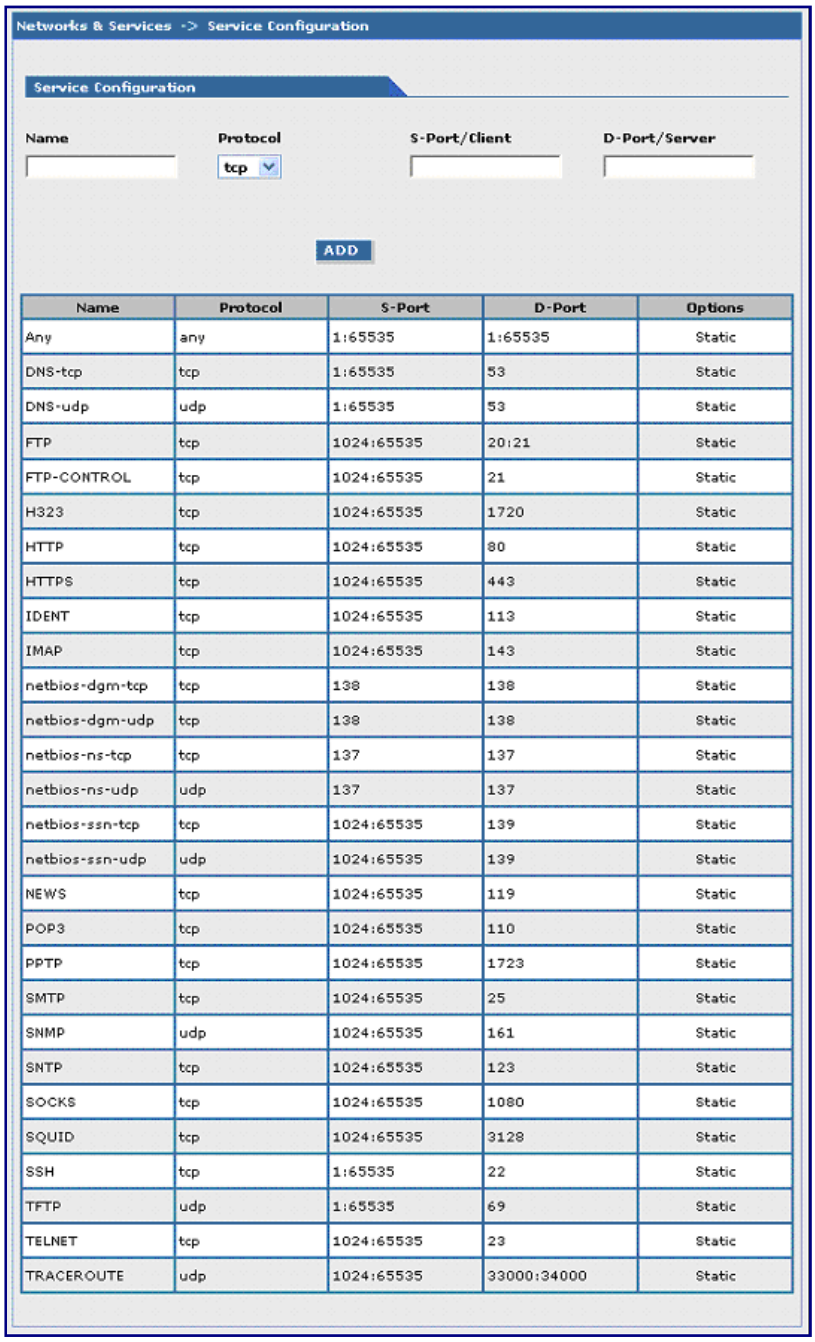
Subnet Mask: Enter the Network Mask of the Network/Host. For Host addresses, the mask is entered as 32.

Note: See *Appendix A -- Table of Commonly Supported Subnets*.

Add Button: Click the **Add** button. The defined network is added and will display at the bottom of the screen.

Networks & Services › Service Configuration

On this screen you can specify the standard set of well known services available on the system. These services enable the configuration of the user-defined services. The options to Delete or Edit a service after it has been defined and added are available by using the table at the bottom of the screen.



Name	Protocol	S-Port	D-Port	Options
Any	any	1:65535	1:65535	Static
DNS-tcp	tcp	1:65535	53	Static
DNS-udp	udp	1:65535	53	Static
FTP	tcp	1024:65535	20:21	Static
FTP-CONTROL	tcp	1024:65535	21	Static
H323	tcp	1024:65535	1720	Static
HTTP	tcp	1024:65535	80	Static
HTTPS	tcp	1024:65535	443	Static
IDENT	tcp	1024:65535	113	Static
IMAP	tcp	1024:65535	143	Static
netbios-dgm-tcp	tcp	138	138	Static
netbios-dgm-udp	tcp	138	138	Static
netbios-ns-tcp	tcp	137	137	Static
netbios-ns-udp	udp	137	137	Static
netbios-ssn-tcp	tcp	1024:65535	139	Static
netbios-ssn-udp	udp	1024:65535	139	Static
NEWS	tcp	1024:65535	119	Static
POP3	tcp	1024:65535	110	Static
PPTP	tcp	1024:65535	1723	Static
SMTP	tcp	1024:65535	25	Static
SNMP	udp	1024:65535	161	Static
SNTP	tcp	1024:65535	123	Static
SOCKS	tcp	1024:65535	1080	Static
SQUID	tcp	1024:65535	3128	Static
SSH	tcp	1:65535	22	Static
TFTP	udp	1:65535	69	Static
TELNET	tcp	1024:65535	23	Static
TRACEROUTE	udp	1024:65535	33000:34000	Static

Service Configuration

Enter the Name, Protocol, Source Port/Client, and Destination Port/Server for the new Service.

- A Service Name cannot be edited.
- A Service cannot be deleted if it is used in another configuration.
- Service changes are reflected in all the configurations in the Web Management software where they are used.
- Services added here will be displayed in the following sections: DNAT, Packet Filters.

Name: Enter the name of the Service which is limited to 16 characters. It has to be unique.

Protocol: Enter the type of protocol (TCP, UDP).

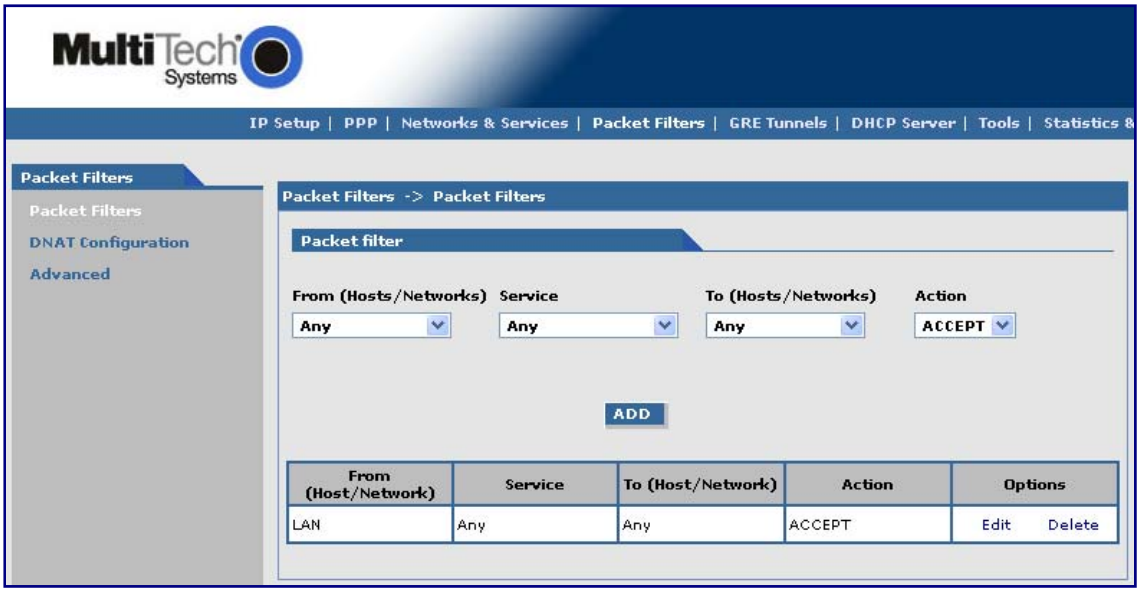
Source Port: Enter the Destination Port for this service. The source and destination ports can be entered either as a single port or a range using a colon as the separator.

Destination Port: Enter the name of the Destination Port for the service.

Add Button: Click the **Add** button. The new service is added and will display on the screen. Packet Filters

Packet Filters › Packet Filters

You can Delete or Edit a packet filter rule after it has been defined and added by using the table at the bottom of the screen.



Packet Filter

From (Host/Networks): Enter the network/host from which the packet must originate for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned addresses or private addresses, may also be entered. The network/host must be pre-defined in the Networks section.

Service: Enter the service that is to be matched with the filter rule. These services must be pre-defined in the Services section. These services precisely define the traffic to be filtered.

To (Host/Networks): Enter the network/host to which the packet must send for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned addresses or private addresses, may also be entered. The network/host must be pre-defined in the Networks section.

Action: Enter the action that the packet filter executes if the rule matches any traffic traversing the firewall. Types of actions defined are:

Accept: Allows/accepts all packets that match this rule.

Reject: Blocks all packets that match this rule. The host sending the packet will be informed that the packet has been rejected.

Drop: Blocks all packets that match this rule, but the host is not informed; i.e., this is a silent drop.

Log: Packets matching the rule; i.e., the corresponding source address, destination address, and service will be logged.

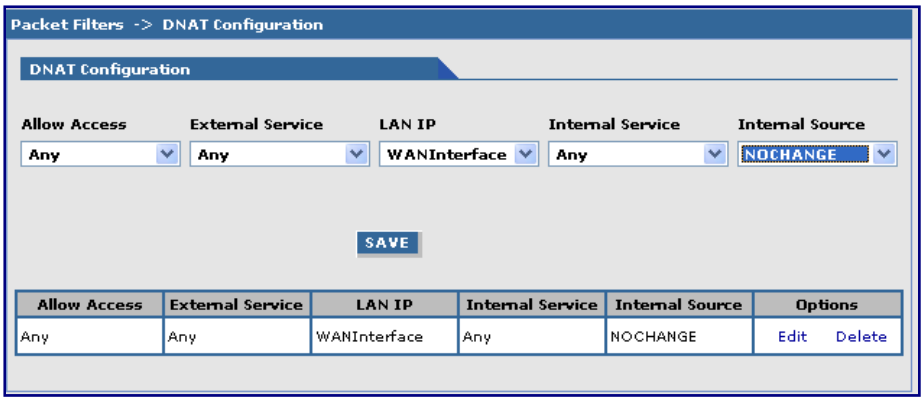
Add Button: Click the **Add** button. The defined packet filter rule is added and will display at the bottom of the screen.

Packet Filters › DNAT Configuration

Destination Network Address Translation (DNAT) is a process that allows the placing of servers within the protected network and making them available for a certain service to the outside world. The DNAT process running on the router translates the destination address of incoming packets to the address of the real network server on the LAN. The packets are then forwarded.

You can Delete or Edit a DNAT rule after it has been defined and added by using the table at the bottom of the screen.

Important Note: When adding rules, at least one host must be defined in the Network Configuration section.



DNAT Configuration

Allow Access: Select a network or host to which IP packets will be allowed and re-routed. The network/host must be pre-defined in the Network Configuration section.

External Service: Select the External Service that you want allowed. The service must be defined in the Service Configuration section.

LAN IP: Select the LAN IP to which the packets are to be diverted. Only one host can be defined as the destination.

Internal Service: Select the Internal Service to be the destination.

Internal Source: Select the source address for packets that going to be sent. If you do not want to change the address, select **NOCHANGE**.

Save Button: Click the **Save** button. The defined DNAT configuration is added and will display at the bottom of the screen. Entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Packet Filters › DNAT Example

Set Up DNAT and Port Forwarding to an Internal Device

Note: The internal device can be camera, meter, security device, etc.

Situation: Assume the device is on a LAN with an IP address of 192.168.2.100 and the port to access the device is port 7700.

1. On the **Network & Services > Network Configuration** screen, set up the following parameters:
   - **Name –** Enter a name for the LAN device.
   - **IP Address and Subnet Address –** Enter the IP address and subnet address of the device.
     - **Example:** Name = MeterIP
       IP Address = 192.168.2.100
       Subnet Address = 255.255.255.255. The subnet mask in the network configuration is not defined using x.x.x.x notation. It uses 'bit' notation. So 255.255.255.255 = 32.
   - **Add –** Click the **Add** button to save this configuration.
2. On the **Network & Services > Service Configuration** screen, define a service name. For this example, the service will be a meter.
   - **Name –** Enter a name for the service (use a name that will identify the service for you).
     - **Example:** MeterPort
   - **Protocol –** Select a protocol.
     - **Example:** tcp/udp
   - **S-Port / Client –** Enter the source port for this service.
     - **Example:** 1:65535
   - **D-Port / Server –** Enter the destination port for this service.
     - **Example:** 7700
   - **Add –** Click the **Add** button to save this configuration.
3. On the **Packet Filters > DNAT Configuration** screen, define the DNAT rule.

Allow Access – Select the original target network/host of the IP packets that you now want rerouted. The original target network/host is the one previously defined in the Network Configuration section.
Example: Any

External Service – Select the External Service that you want allowed. The service must be defined in the Service Configuration section.

LAN IP – Select the LAN IP to which the packets are to be diverted. Only one host can be defines as the destination.

Internal Service – Select the Internal Service to be the destination.

Pre DNAT Service – Select the service for the Pre-DNAT destination. This service was just defined in the Service Configuration section.
Example: MeterPort

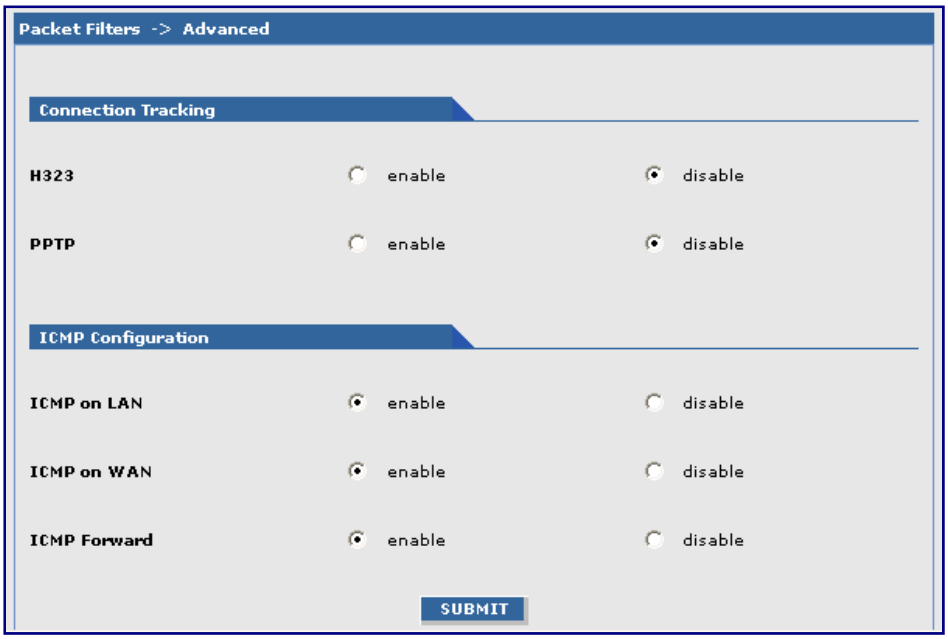
Post DNAT IP – Select the destination to which the IP packets are to be diverted. Only one host can be defined as the Post DNAT destination.
Example: MeterIP

Post DNAT Service – Select the service for the Post DNAT configuration.
Example: MeterPort

Internal Source – Select the source address for packets that going to be sent. If you do not want to change the address, select **NOCHANGE**.
Example: NOCHANGE

4. **Save –** Click the **Save** button to save this configuration.
Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Packet Filters › Advanced



Connection Tracking

H323: Enable/disable the forwarding of H323 packets across the firewall.

PPTP: Enable/disable PPTP Packet Pass-through (PPTP NAT support).

ICMP Configuration

The Internet Control Message Protocol (ICMP) is used to test the network connections and the functionality of the firewall and is also used for diagnostic purposes. *ICMP on Firewall* and *ICMP Forwarding* always apply to all IP addresses; i.e., *Any*. When these are enabled, all IP hosts can Ping the firewall (*ICMP on Firewall*) or the network behind it (*ICMP Forwarding*).

ICMP on LAN: Enable/disable the transfer of ICMP packets on the LAN interface.

ICMP on WAN: Enable/disable the transfer of ICMP packets on the WAN interface.

ICMP Forward: Enable/disable the forwarding of ICMP packets through the firewall into the local network.

Submit

Click the **Submit** button to save these settings.

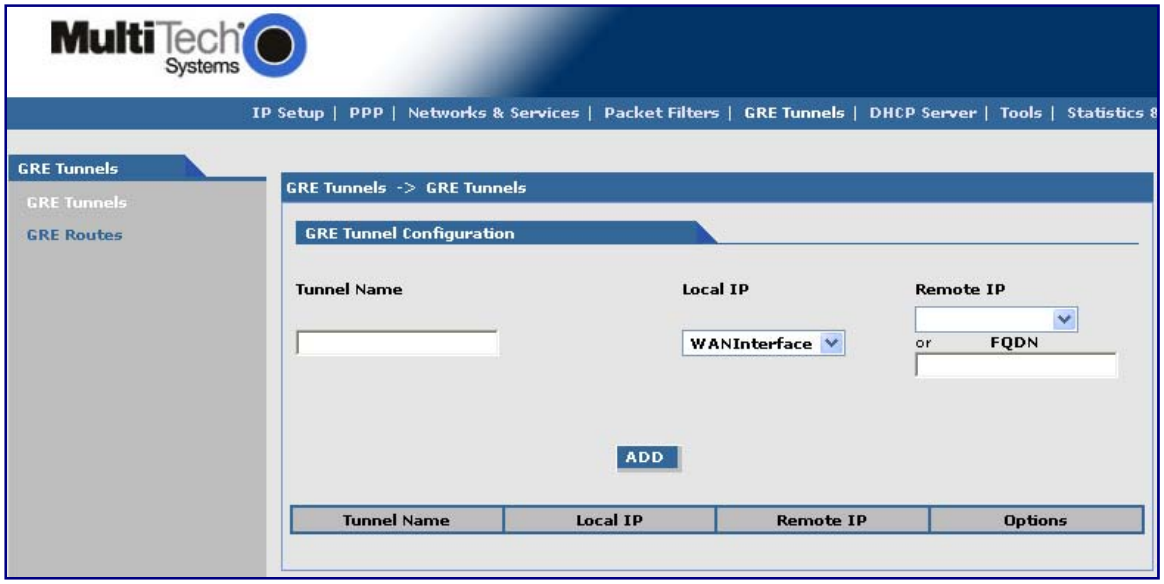
Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

GRE Tunnels

GRE tunneling and GRE routing together are referred to Generic Routing Encapsulation (GRE). GRE Routing is an integral part of GRE tunneling. First, the GRE Tunnels are created using the GRE Tunnel Configuration. Then the routes for the remote networks that are to be routed through a tunnel need to be specified in the GRE Routes Configuration. Thus, all the traffic destined to remote networks associated to a tunnel will get routed through that tunnel.

GRE Tunnels › GRE Tunnels

Tunneling allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols. If you want to read more about how this works, see the online Help.



GRE Tunnel Configuration

Tunnel Name: Enter a name for the new tunnel.

Local IP: Select the local interface on which the tunnel is being created. Eventually, the packets destined for this tunnel will be routed through it.

Note: When adding a tunnel, use only one of the following: **Remote IP** or **FQDN**.

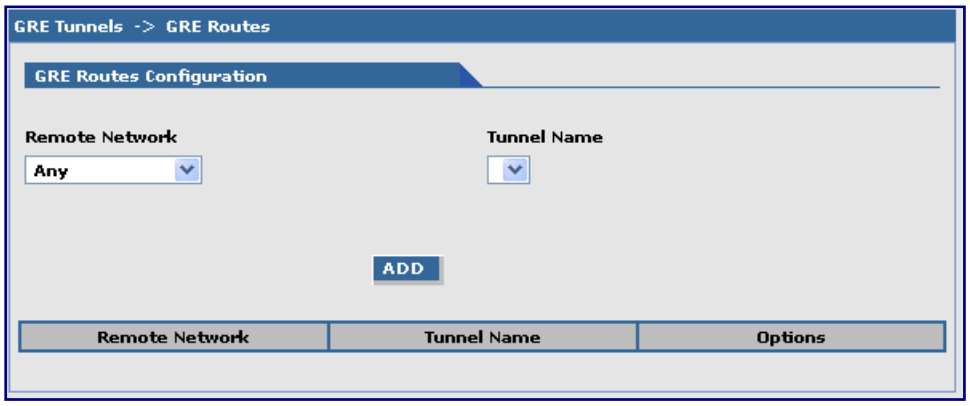
Remote IP: Select the Remote IP address that marks the other end point of the tunnel (this is the one to which the routed packets will be received).

OR

FQDN: Enter the FQDN (Fully Qualified Domain Name) for the Remote IP, which can be either the IP Address of an FQDN.

Add Button: Click the **Add** button. The defined GRE tunnel configuration is added and will display at the bottom of the screen.

GRE Tunnels › GRE Routes Configuration



GRE Routes Configuration

Remote Network: Select the remote network for which the traffic destined to it must be routed through the given tunnel.

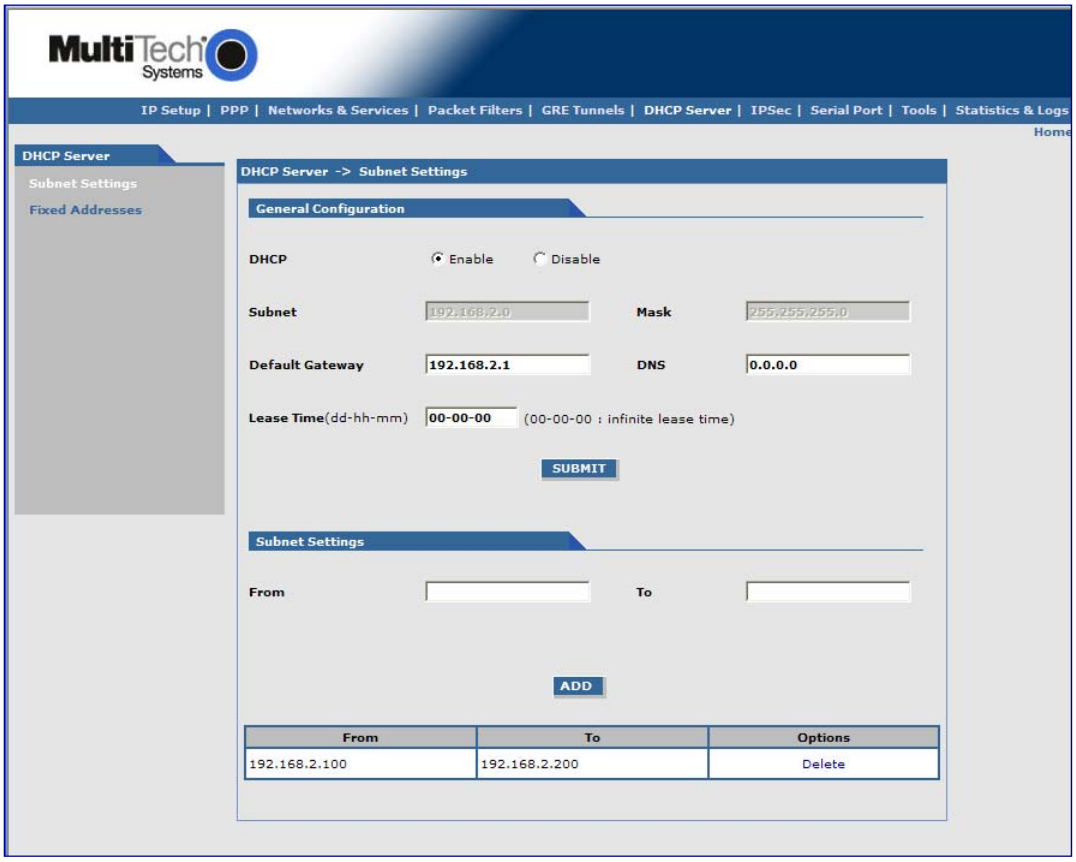
Tunnel Name: Select the name of the tunnel through which the traffic will be routed.

Note: To add a tunneled route, the remote network and the tunnel must have been defined in Network Configuration. The tunnel configuration must be completed before setting the GRE route configuration.

Add Button: Click the **Add** button. The defined GRE route configuration is added and will display at the bottom of the screen.

DHCP Server

DHCP Server › Subnet Settings



General Configuration

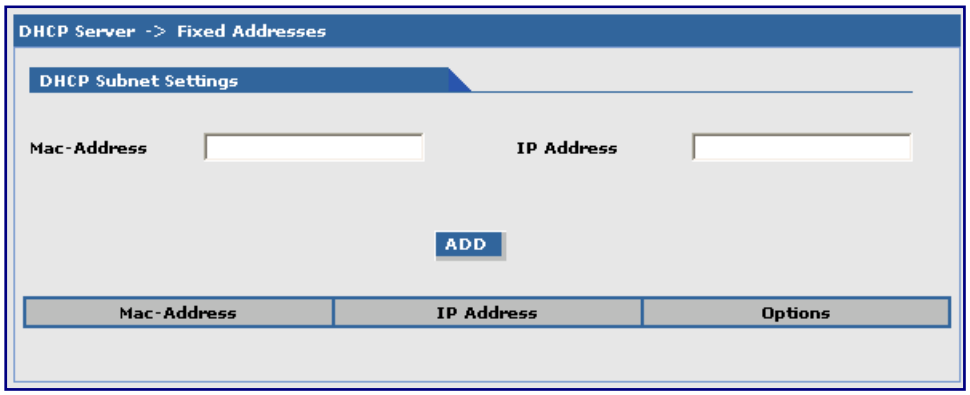
DHCP (Dynamic Host Configuration Protocol) is a protocol that allows individual devices on an IP network to get their own network configuration information (IP address, subnet mask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network.

DHCP:	Enable/disable the DHCP server.
Subnet:	Enter the subnet address. If you want to change the DHCP subnet address, you first have to delete all the subnet settings below.
Mask:	Enter the subnet mask.
Gateway:	Enter the gateway address.
DNS:	Enter the DNS address.
Lease Time:	Select the DHCP Lease Time from the selection box. Lease time is set in days, hours, and minutes. A Lease Time of 00-00-00 is an Infinite Lease Time.
Submit	Click the **Submit** button to save these settings.
	Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

Subnet Settings

From-To Range:	Enter the range of IP addresses to be assigned by DHCP.
Add:	Click the **Add** button. The address range is added and will display in the table at the bottom of the screen. Once the range displays, you can delete if necessary.
Note:	See *Appendix A – A Table of Commonly Supported Subnets*.

DHCP Server › Fixed Addresses



DHCP Fixed Configuration

The DHCP server can be made to assign a fixed IP address for a particular user by identifying the MAC address. This binding can be made permanent by configuring it here. The same IP address will not be used for any DHCP client with a different MAC address, even if there is no active DHCP connection with that IP address.

MAC Address: Enter the MAC address to which the specified IP address binds.

IP Address: Enter the fixed IP address to be assigned.

Add: Click the **Add** button. The addresses are added and will display in the table at the bottom of the screen from where they can be deleted or changed.

IPSec

The IPSec (IP Security) protocol suite, based on modern cryptographic technologies, provides security services like encryption and authentication at the IP network layer. It secures the whole network traffic providing guaranteed security for any application using the network. It can be used to create private secured tunnels between two hosts, two security gateways, or a host and a security gateway. Up to four tunnels can be active at any given time. Beyond four active tunnels can be saved, but they will not be active.

IPSec provides encryption and authentication services at the IP level of the protocol stack. IPSec can protect any traffic carried over IP.

IPSec provides the following services:

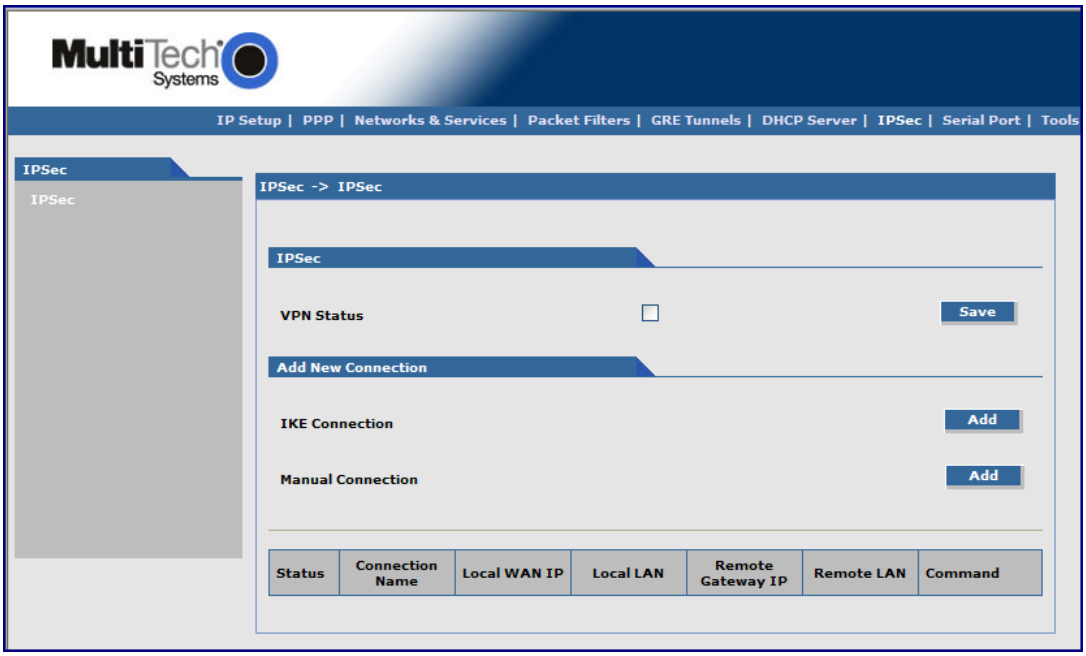
- Authentication only
- Encryption only
- Authentication and encryption

Transmitting and receiving data securely over an unprotected network involves deciding on the type of IPSec service, as mentioned above, required for the connection, establishing a secure connection by a key exchange process and transferring data using that connection.

The key exchange process is done in one of two ways:

1. Manual Keying where the authentication and encryption keys are provided manually on both sides of the connection.
2. Auto Keying using IKEv2 Protocol where the authentication and encryption keys are generated on either side of the connection and exchanged by different methods.

IPSec › IPSec



IPSec

VPN Status Check the VPN *Status* checkbox to enable IPSec. Click the **Save** button.

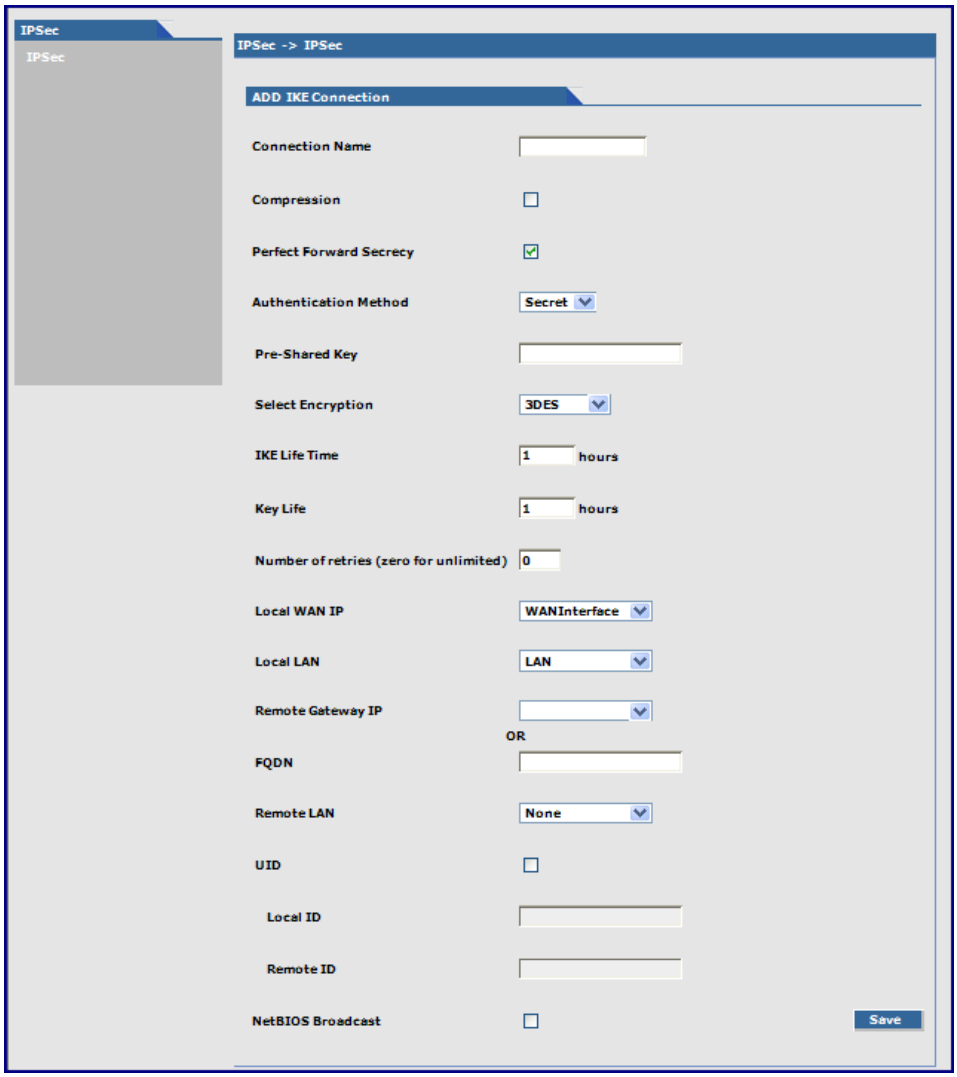
Add a New Connection

Add IKE Connection Click the *Add IKE Connection* button. A screen displays for setting up an IKE connection.

Add Manual Connection Click the *Add Manual Connection* button. A separate screen displays for setting up a manual connection.

Important Note About Activating a Connection: Once connection information is entered, it will display at the bottom of this screen. Be sure to check the box in the **Status** column to activate the connection.

Add IKE Connection



Add an IKE Connection

Connection Name Enter a text name that will identify the connection for you.

Compression Check the compression checkbox to enable IPCOMP, the compression algorithm.

Perfect Forward Secrecy (PFS) Check the PFS checkbox to enable PFS, a concept in which the newly generated keys are unrelated to the older keys). This is enabled by default.

Authentication Method Authentication can be done using Pre-Shared Secrets.

Pre-Shared Key The Pre-Shared Key must be agreed upon and shared by the VPN endpoints; it must be configured at both endpoints of the tunnel.

Select Encryption Select the encryption method. 3DES is recommended. Options include: 3DES, AES-128, AES-192, AES-256

IKE Life Time The duration for which the ISAKMP SA should last is from successful negotiation to expiration. The default value is one hour and the maximum is 8 hours.

Key Life The duration for which the IPSec SA should last is from successful negotiation to expiration. The default value is one hour and the maximum is 24 hours.

Number of Retries Specify the number of retries for the IPSec tunnel. Enter zero for unlimited retries.

Local WAN IP This is the interface initiating the IPSec tunnel.

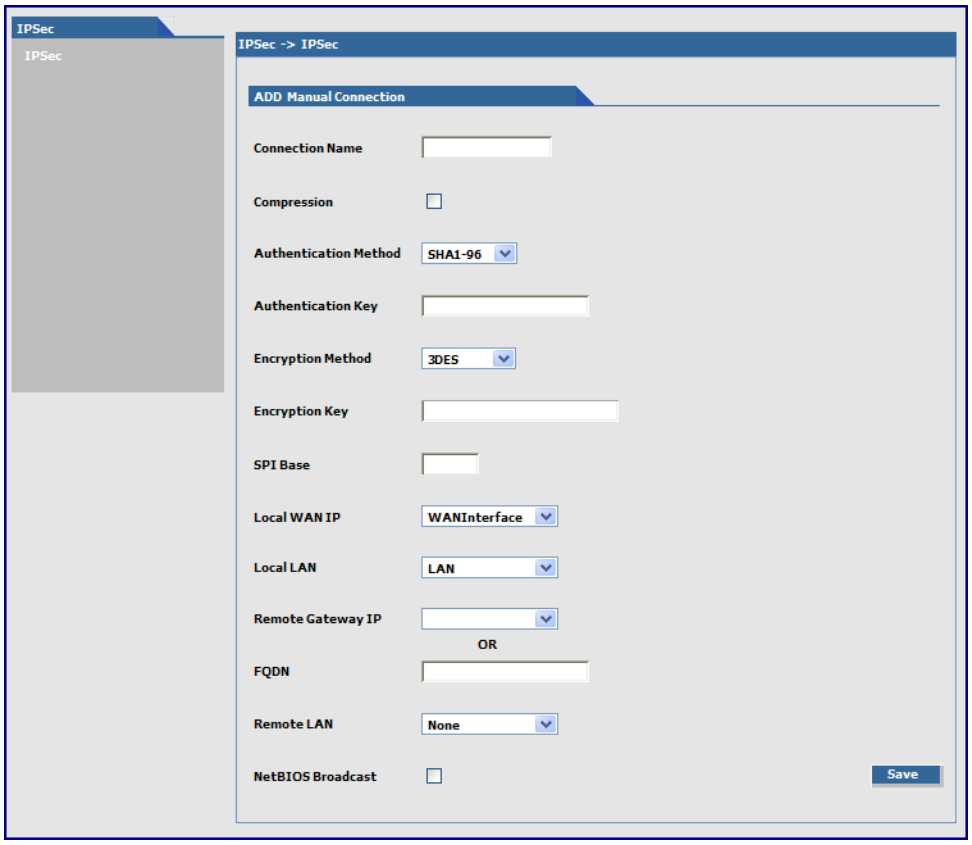
Local LAN Internal subnet of the local security gateway for which the security services should be provided. If the RouteFinder acts as a host, this should be configured as None.

Remote Gateway IP	Interface where the IPSec tunnel ends. In the case of a Road Warrior with a Dynamic IP address, this should be configured to **ANY**.
FQDN	FQDN is a DNS resolvable fully qualified domain name with which identity the right peer can be identified. When FQDN is selected, the Remote Gateway IP should be blank.
Remote LAN	Internal subnet of the remote security gateway for which the security services should be provided. If the remote end is the host, this should be configured as None.
UID (Unique Identifier String)	Check the UID box to enable the Local ID and Remote ID. Local ID and Remote ID are active only when UID is enabled. ***Local ID*** Enter a string identifier for the local security gateway. ***Remote ID*** Enter a string identifier for the remote security gateway.
NetBIOS Broadcast	Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

Save Button

Click the Save button to save these settings.

Add Manual Connection



Add Manual Connection

Connection Name Enter a text name that will identify the connection for you.

Compression Check the compression checkbox to enable IPCOMP, the compression algorithm.

Authentication Method Select the authentication algorithms to be used for the respective security services. Options are: MD5-96 and SHA1-96.

Authentication Key The VPN firewall could use either MD5-96 or SHA1-96 for authentication. For example, MD5-96 could have a key of abcdefgh12345678.

Authentication Protocol	Key Length	Accepted Characters
SHA1-96	Must be 20 characters	Alphanumeric characters
MD5-96	Must be 16 characters	Alphanumeric characters

Encryption Method Select the encryption method. Options include: 3DES, AES-128, AES-192, AES-256, and NULL (no encryption).

Encryption Key The RouteFinder can use any one of the methods specified in its encryption algorithm. For example 3DES uses 24 alphanumeric characters (192 bits) as its encryption key. Example: 1234567890abcdefabcdabcd

Encryption Protocol	Key Length	Accepted Characters
Null	Must be 24 characters	Alphanumeric Characters
3DES	Must be 24 characters	Alphanumeric Characters
AES-128	Must be 16 characters	Alphanumeric Characters
AES-192	Must be 24 characters	Alphanumeric Characters
AES-256	Must be 32 characters	Alphanumeric Characters

SPI Base The Security Parameter Index identifies a manual connection. The SPI is a unique identifier in the SA (Secure Association – a type of secure connection) that allows the receiving computer to select the SA under which a packet will be processed. The SPI Base

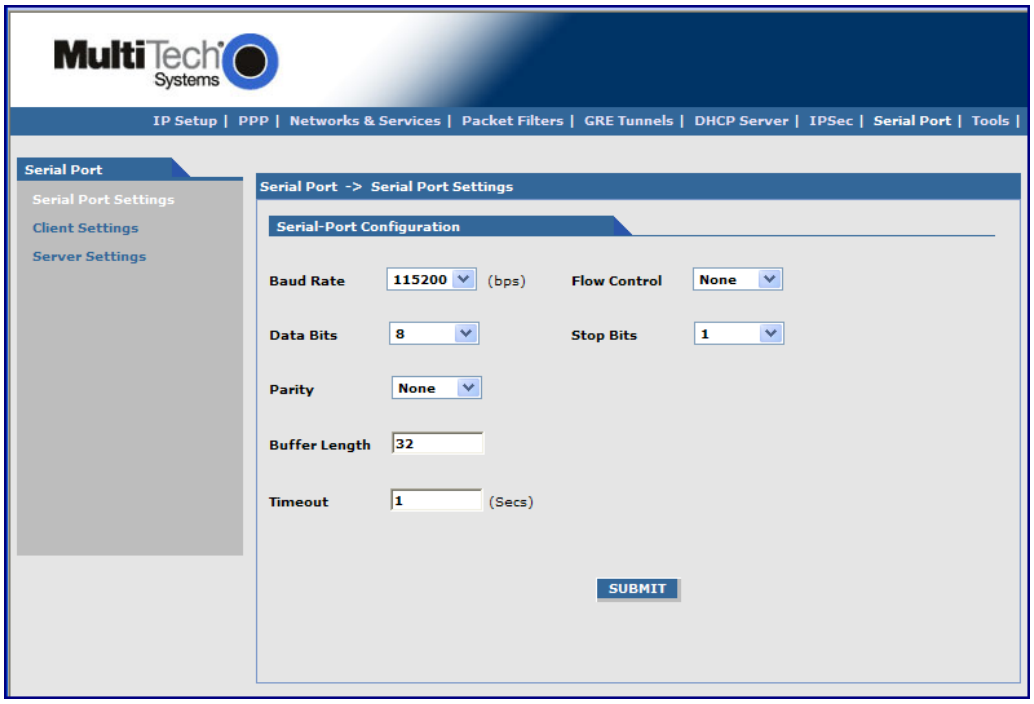
	is a number needed by the manual keying code. Enter any 3-digit hexadecimal number, which is unique for a security association. It should be in the form 0xhex (0x100 through 0xfff is recommended). If you have more than one manual connection, then the SPI Base must be different for each one.
Left Next Hop	*Next Hop* is the address of the next device in a routing table's path that moves a packet to it's destination. This setting can be configured or left as a static value: 0.0.0.0. When not configured, the value is set to the Gateway of the Box/Gateway configured on the Interface/Right IP. The selection is based on the Left and Right IP.
Local WAN IP	Select the Interface to initiate the IPSec tunnel (Left Security Gateway).
Local LAN	Select the internal subnet of the local security gateway for which the security services are to be provided. If the RouteFinder acts as a host, this should be configured as **None**. Other options are: Any, LAN, LAN Interface, WAN 1, WAN 1 Interface.
Remote Gateway IP	Select the interface in which the IPSec tunnel ends. In the case of Road Warriors with a Dynamic IP addresses, this should be configured as **ANY**. Other options include: LAN, LAN Interface, WAN 1, WAN 1 Interface, and None.
FQDN	FQDN is a DNS resolvable fully qualified domain name with which identity the right peer can be identified. When FQDN is entered, the Remote Gateway IP should be blank.
Remote LAN	This is the internal subnet of the remote security gateway for which the security services are to be provided. If the remote end is a host, this should be configured as **None**.
NetBIOS Broadcast	Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

Save Button

Click the Save button to save these settings.

Serial-Port

Serial-Port › Serial Port Settings



Serial-Port Configuration

Serial-Port Configuration allows for the configuration of the serial terminal connected to the RS-232 connector DE9 on the back of the unit.

Baud Rate: Sets the baud-rate at which the serial terminal will be communicating. The default is 115200.

Flow Control: Sets the flow control for the serial port. The selections are None or RTS-CTS. The default is None.

Data Bits: Sets the data bits for the serial port. Data bit selection is 7 or 8. The default is 8.

Stop Bits: Sets the stop bits for the serial port. The selections are 1 or 2. The default is 1.

Parity: Sets the parity for the serial port. The selections are None, Even, or Odd. The default is None.

Buffer Length: Sets the length up to which the data from the serial device is buffered before IP transmission. The default length is 32-characters.

Timeout: Sets the timeout value for the serial terminal of how long it should wait before IP transmission, The default is 1-second.

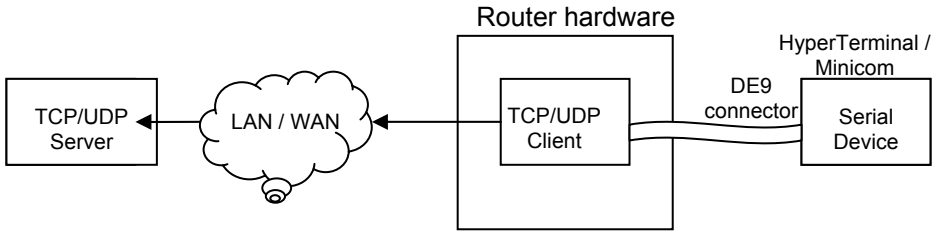
Submit Button

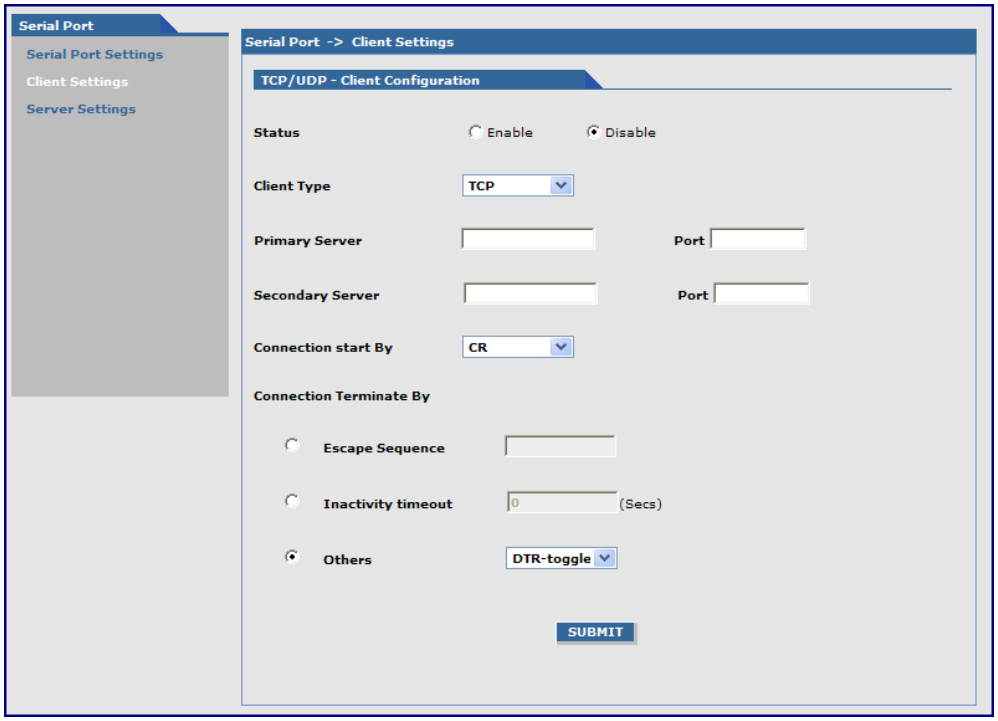
Click the Submit button to save these settings.

Serial Port › Client Settings

The TCP/UDP client feature enables the router to act as a proxy TCP/UDP client to the serial terminal connected to the DE9, RS232 port on the router thus facilitating the serial terminal to access any TCP/UDP server on the LAN/WAN. Once the session, serial terminal to TCP/UDP server, is opened successfully, it allows two-way traffic between the serial device and the remote server.

Initial connection setup for the TCP/UDP client is as shown below:





TCP/UDP – Client Configuration

Configures TCP/UDP Client through which the serial terminal connected to the RS-232 connector, DE9 on the back of the unit communicates with the remote TCP/UDP server on the LAN/WAN.

Status: Sets the client status to either Enable or Disable. The default is Disable

Client Type: Sets the client to either TCP or UDP. The default is TCP.

Primary Server: Enter the Primary Server IP address or Hostname. The default is blank.

Secondary Server: Enter the Secondary Server IP address or Hostname. The default is blank.

Connection start By: Sets the trigger in the serial port by which the connection starts. The default is Carriage Return (CR).

Connection Terminate By: Sets the connection terminate sequence as follows:

Escape Sequence: Set the escape sequence characters at which the connection should terminate.

Inactivity timeout: Set the inactivity timeout at which the connection should terminate.

Others: The other terminating sequences are: DTR-toggle or Always-On.

DTR-toggle: If DTR status goes low, the connection terminates.

Always-On: Sets the terminate sequence as Always-on.

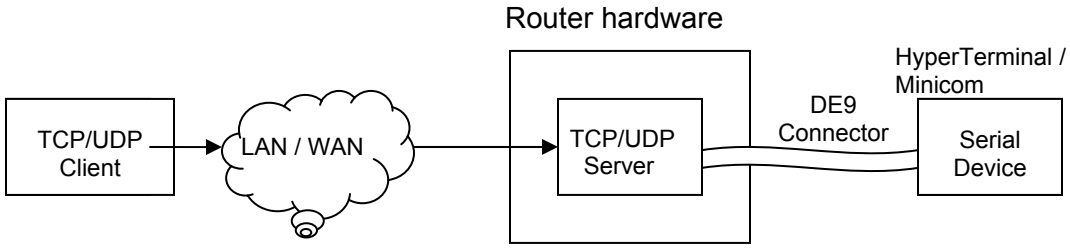
Submit Button

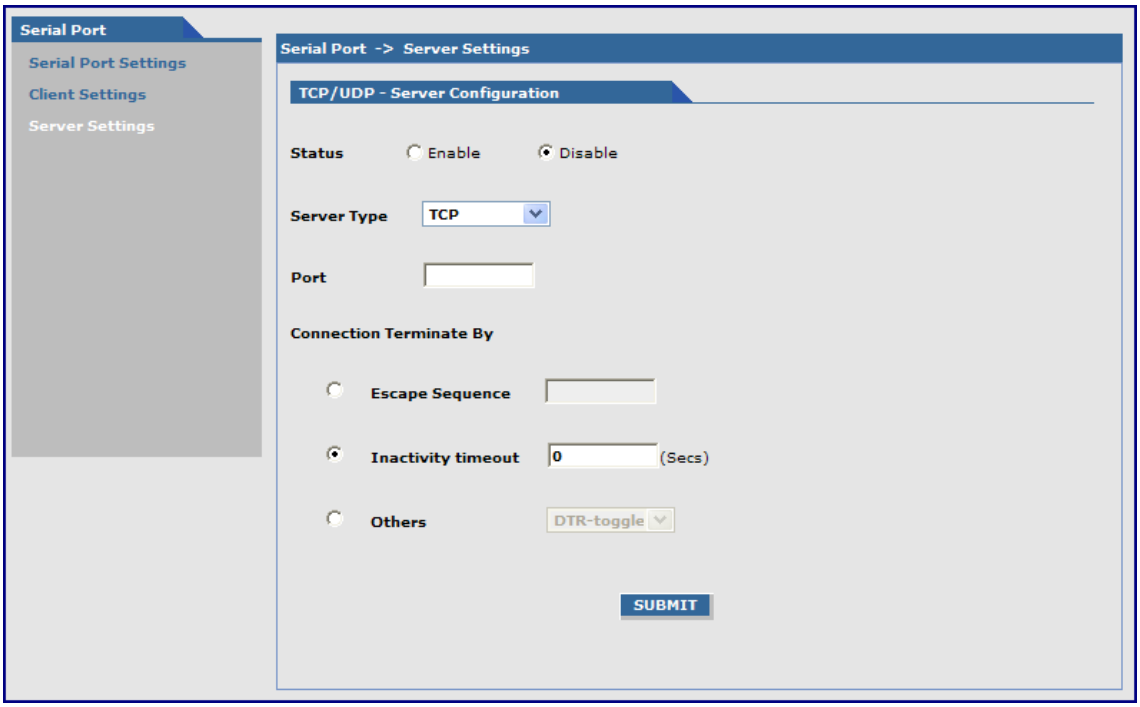
Click the Submit button to save these settings.

Serial Port > Server Settings

This feature enables a TCP/UDP client on the Ethernet network to connect to the remote serial terminal connected to the DE9, RS232 port on the router. The router acts as a TCP/UDP server which allows two way traffic between the TCP/UDP client and the remote terminal on the serial port.

The initial connection setup for the TCP/UDP server is as shown below.





TCP/UDP – Server Configuration

Configures TCP/UDP Server through which the serial terminal connected to the RS-232 connector, DE9 on the back of the unit listens for the remote TCP/UDP client to communicate on the LAN/WAN.

Status: Sets the client status to either Enable or Disable. The default is Disable

Server Type: Sets the client to either TCP or UDP. The default is TCP.

Port: Sets the server port. The default is None

Connection Terminate By: Sets the connection terminate sequence as follows:

Escape Sequence: Set the escape sequence characters at which the connection should terminate.

Inactivity timeout: Set the inactivity timeout at which the connection should terminate.

Others: The other terminating sequences are: DTR-toggle or Always-On.

DTR-toggle: If DTR status goes low, the connection terminates.

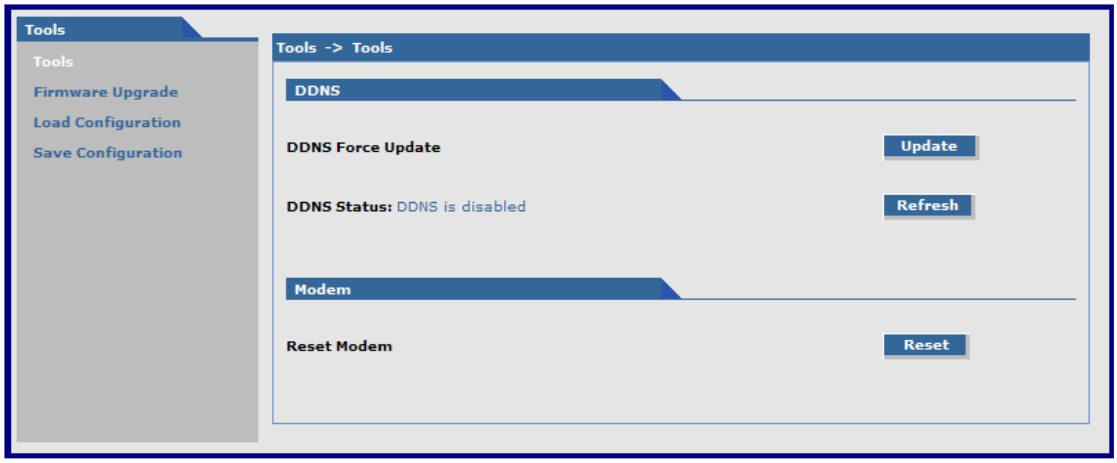
Always-On: Sets the terminate sequence as Always-on.

Submit Button

Click the Submit button to save these settings.

Tools

Tools › Tools



DDNS

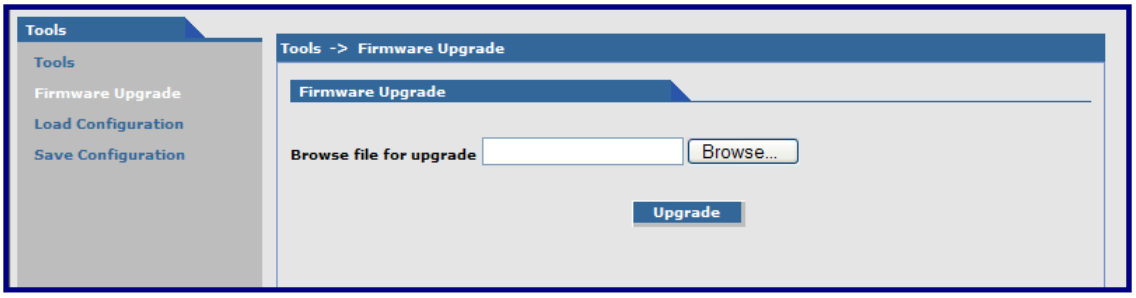
DDNS Force Update: Click the **Update** button to update the DDNS server with your current dynamically assigned IP address.

DDNS Status: Click the **Refresh** button to display the DDNS Status after a forced update.

Modem

Reset Modem: Click the **Reset** button to reset the integrated cellular modem.

Tools › Firmware Upgrade



Firmware Upgrade

The firmware for the router can be upgraded to the latest version using this feature. All Multi-Tech firmware upgrades are posted on the Multi-Tech Web site from which they can be downloaded.

Note: Before you upgrade your firmware, you should save your present configuration. After the firmware upgrade is complete, you should verify your configuration to ensure that it is as expected. Particularly, check that the DHCP scope settings are set properly.

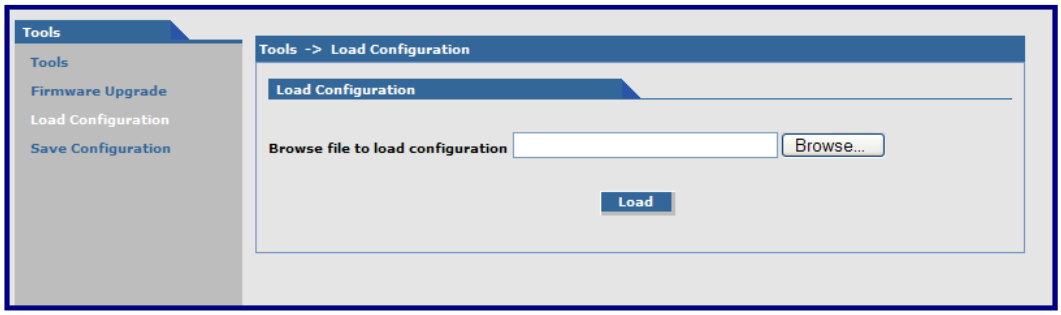
Browse File for Upgrade: Click the **Browse** button and locate the latest firmware version to be downloaded. Select the **mtcba-en2-u-xxx.bin** file. Highlight the file name and press **Enter** so that the file name displays in the text box. Make sure you select the correct BIN file; otherwise, your router can become inoperable. Then click the **Upgrade** button.

When upgrade is completed, the program will return to the main login screen.

Important Notes:

- The new firmware is written into the flash.
- A **Firmware Upgrade** will take at least 4 minutes while the firmware is downloaded. Do not cycle power during this time.
- **DO NOT** perform firmware upgrade remotely via the Cellular wireless connection.

Tools › Load Configuration



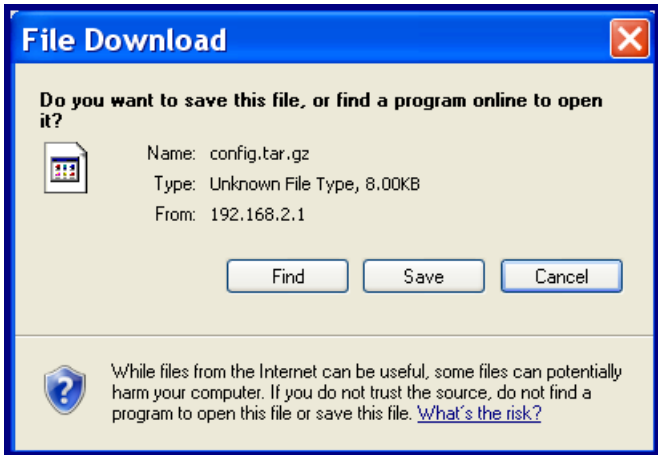
Load Configuration

Browse File for Load Configuration: Click the **Browse** button to open the file that allows you to locate the configuration file. When found, highlight the file name and press Enter so that the file name displays in the text box. Then click the **Load** button.

Important Notes:

- The new configuration is written into the flash.
- A **Configuration Upgrade** will take at least 3 seconds to download and 60 seconds to install the settings and reboot. Reboot happens automatically.

When you click the **Load** button, the following screen displays. It shows the name of the file you selected.


File Download
Do you want to save this file, or find a program online to open it?
Name: config.tar.gz
Type: Unknown File Type, 8.00KB
From: 192.168.2.1
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

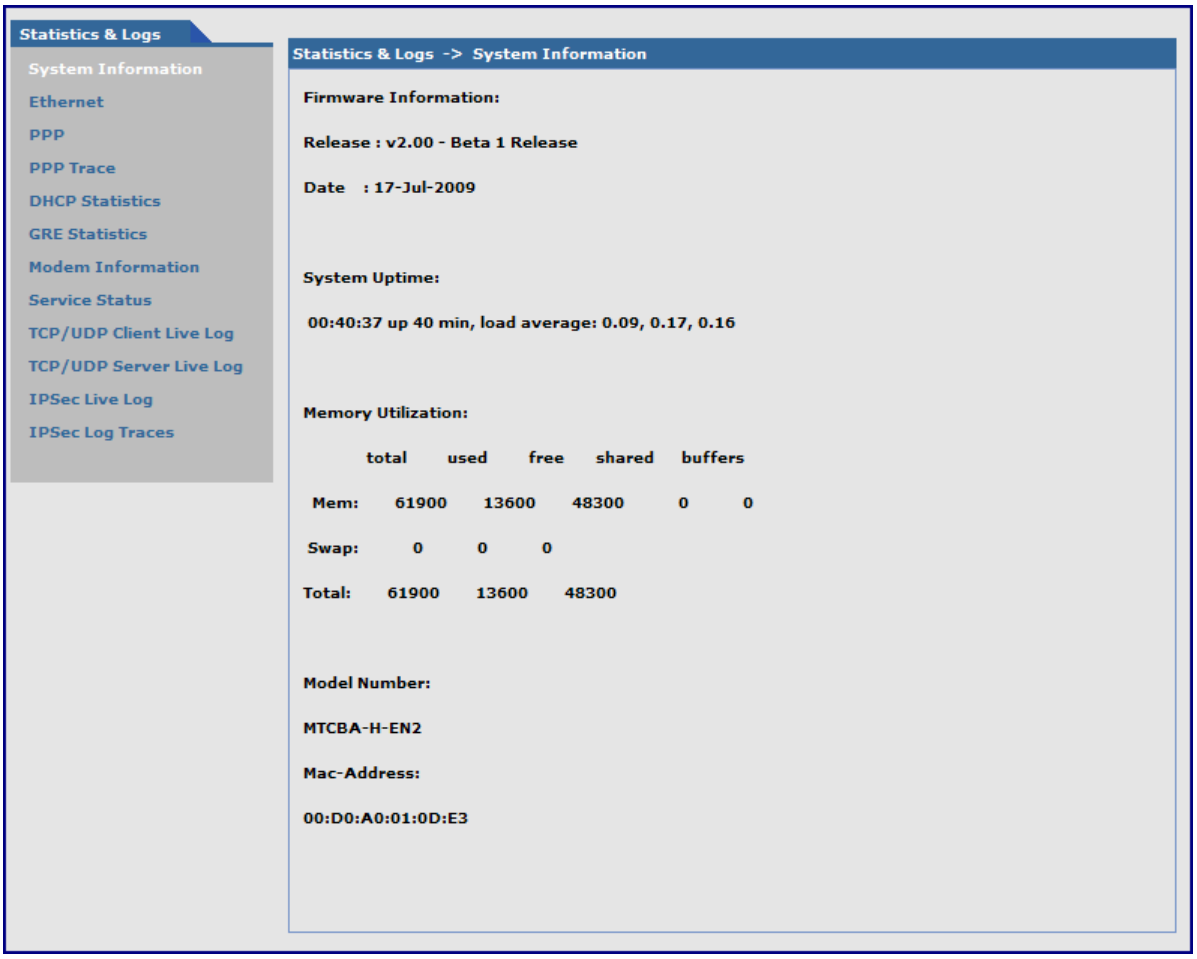
Click the **Find**, **Save**, or **Cancel** buttons as desired. The **More Info** displays Microsoft's Internet Explorer Help on downloading files.

Tools > Save Configuration

Click this option to save the configuration.

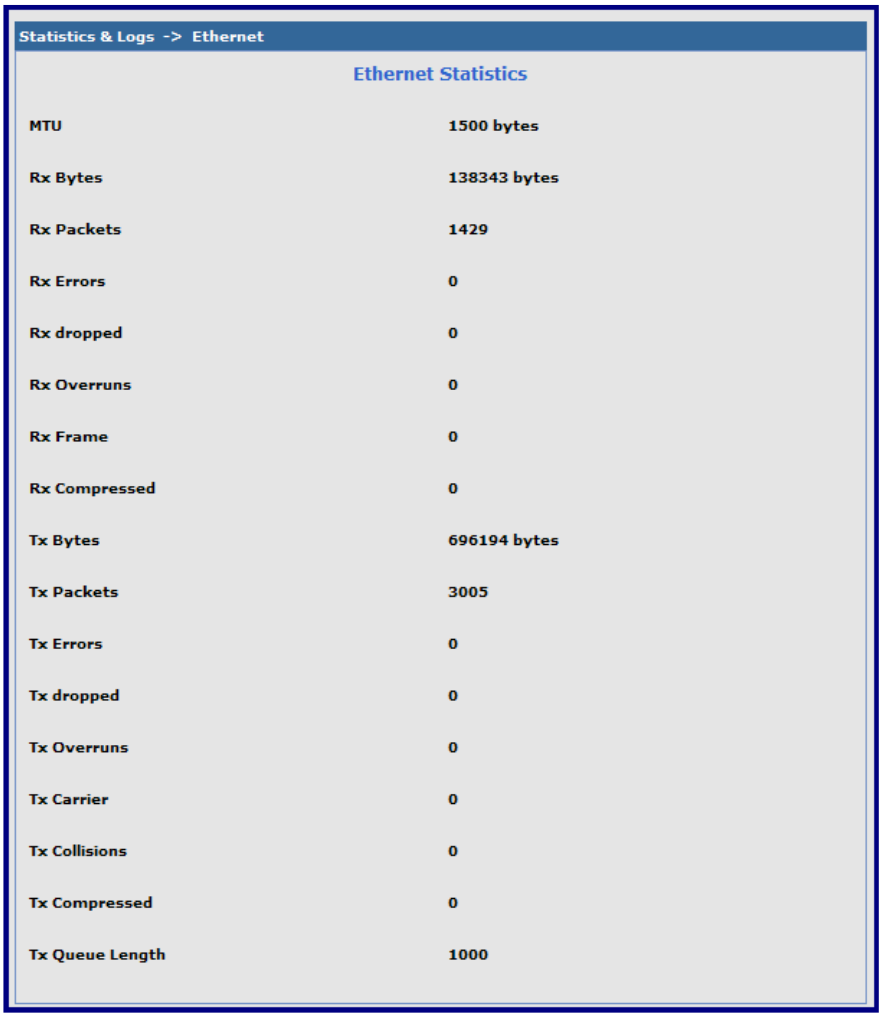
Statistics & Logs

Statistics & Logs > System Information



This is an example of the Statistics & Logs System Information

Statistics & Logs > Ethernet



This is an example of the Ethernet Statistics & Logs screen. It shows Ethernet statistics.

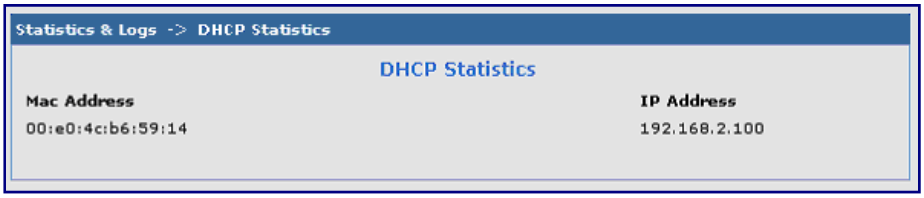
Statistics & Logs > PPP

This is an example of the PPP Statistics & Logs screen. It shows PPP statistics when PPP is enabled.

Statistics & Logs > PPP Trace

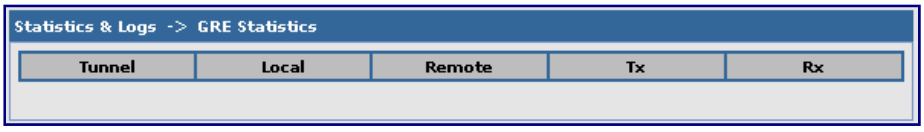
This is an example of the PPP Trace Statistics & Logs screen. It shows the PPP trace messages.

Statistics & Logs > DHCP Statistics



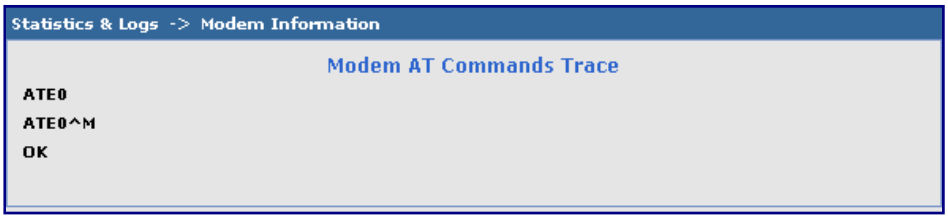
This is an example of the DHCP Statistics & Logs screen. It shows the statistics of DHCP leases.

Statistics & Logs > GRE Statistics



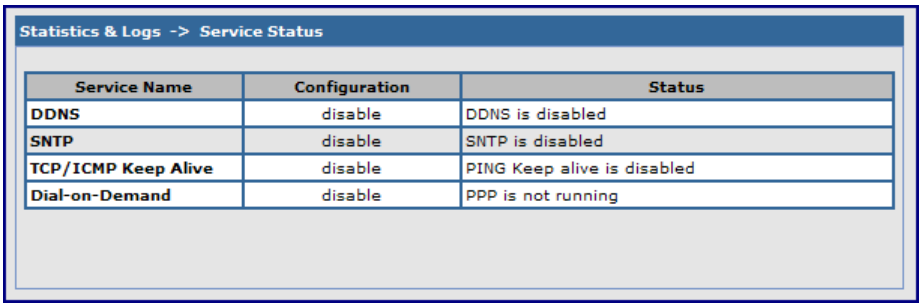
This screen displays the statistics of active tunnels.

Statistics & Logs > Modem Information

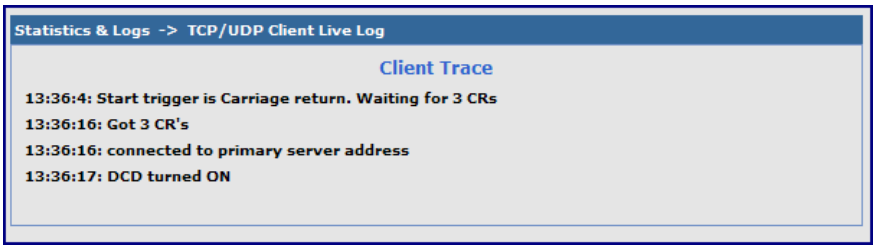


This screen displays the modem commands set on the **PPP > Modem Commands** screen and also displays the results of the commands.

Statistics & Logs > Service Status

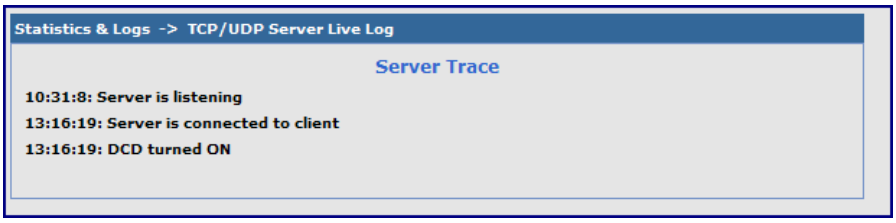


Statistics & Logs > TCP/UDP Client Live Log


Statistics & Logs -> TCP/UDP Client Live Log
Client Trace
13:36:4: Start trigger is Carriage return. Waiting for 3 CRs
13:36:16: Got 3 CR's
13:36:16: connected to primary server address
13:36:17: DCD turned ON

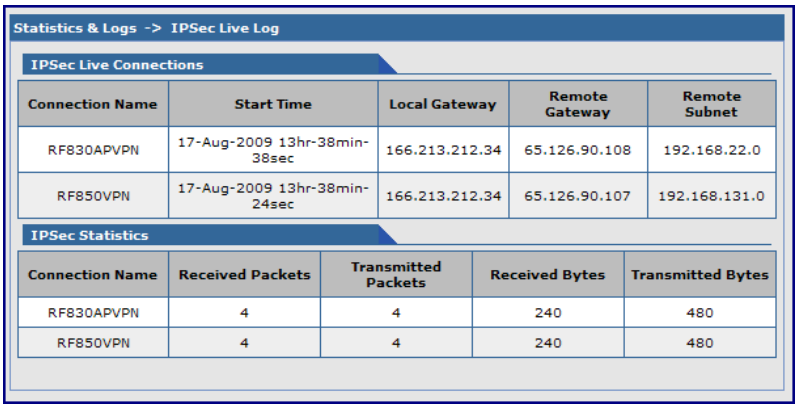
This screen displays the TCP/UDP Client Live Log.

Statistics & Logs > TCP/UDP Server Live Log


Statistics & Logs -> TCP/UDP Server Live Log
Server Trace
10:31:8: Server is listening
13:16:19: Server is connected to client
13:16:19: DCD turned ON

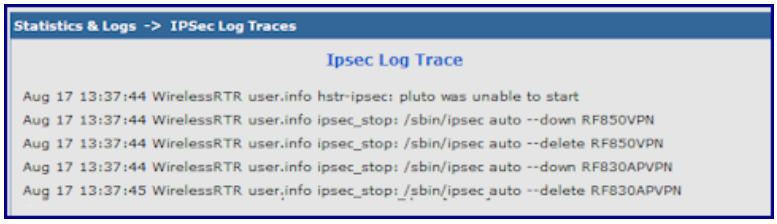
This screen displays the TCP/UDP Server Live Log.

Statistics & Logs > IPSec Live Log



This screen displays the IPSec Live Log.

Statistics & Logs > IPSec Log Traces


Statistics & Logs -> IPSec Log Traces
Ipsec Log Trace
Aug 17 13:37:44 WirelessRTR user.info hstr-ipsec: pluto was unable to start
Aug 17 13:37:44 WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --down RF850VPN
Aug 17 13:37:44 WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --delete RF850VPN
Aug 17 13:37:44 WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --down RF830APVPN
Aug 17 13:37:45 WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --delete RF830APVPN

This screen displays the IPSec Log Traces.

Appendix A – A Reference Table of Commonly Supported Subnets

This table lists commonly supported Subnets organized by Address.

	Network Number	Hosts Available	Broadcast Address
255.255.255.128	N.N.N.0	N.N.N.1-126	N.N.N.127
/25	N.N.N.128	N.N.N.129-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.192	N.N.N.0	N.N.N.1-62	N.N.N.63
/26	N.N.N.64	N.N.N.65-126	N.N.N.127
	N.N.N.128	N.N.N.129-190	N.N.N.191
	N.N.N.192	N.N.N.193-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.224	N.N.N.0	N.N.N.1-30	N.N.N.31
/27	N.N.N.32	N.N.N.33-62	N.N.N.63
	N.N.N.64	N.N.N.65-94	N.N.N.95
	N.N.N.96	N.N.N.97-126	N.N.N.127
	N.N.N.128	N.N.N.129-158	N.N.N.159
	N.N.N.160	N.N.N.161-190	N.N.N.191
	N.N.N.192	N.N.N.193-222	N.N.N.223
	N.N.N.224	N.N.N.225-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.240	N.N.N.0	N.N.N.1-14	N.N.N.15
/28	N.N.N.16	N.N.N.17-30	N.N.N.31
	N.N.N.32	N.N.N.33-46	N.N.N.47
	N.N.N.48	N.N.N.49-62	N.N.N.63
	N.N.N.64	N.N.N.65-78	N.N.N.79
	N.N.N.80	N.N.N.81-94	N.N.N.95
	N.N.N.96	N.N.N.97-110	N.N.N.111
	N.N.N.112	N.N.N.113-126	N.N.N.127
	N.N.N.128	N.N.N.129-142	N.N.N.143
	N.N.N.144	N.N.N.145-158	N.N.N.159
	N.N.N.160	N.N.N.161-174	N.N.N.175
	N.N.N.176	N.N.N.177-190	N.N.N.191
	N.N.N.192	N.N.N.193-206	N.N.N.207
	N.N.N.208	N.N.N.209-222	N.N.N.223
	N.N.N.224	N.N.N.225-238	N.N.N.239
	N.N.N.240	N.N.N.241-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.248	N.N.N.0	N.N.N.1-6	N.N.N.7
/29	N.N.N.8	N.N.N.9-14	N.N.N.15
	N.N.N.16	N.N.N.17-22	N.N.N.23
	N.N.N.24	N.N.N.25-30	N.N.N.31
	N.N.N.32	N.N.N.33-38	N.N.N.39
	N.N.N.40	N.N.N.41-46	N.N.N.47
	N.N.N.48	N.N.N.49-54	N.N.N.55
	N.N.N.56	N.N.N.57-62	N.N.N.63
	N.N.N.64	N.N.N.65-70	N.N.N.71
	N.N.N.72	N.N.N.73-78	N.N.N.79
	N.N.N.80	N.N.N.81-86	N.N.N.87
	N.N.N.88	N.N.N.89-94	N.N.N.95
	N.N.N.96	N.N.N.97-102	N.N.N.103
	N.N.N.104	N.N.N.105-110	N.N.N.111
	N.N.N.112	N.N.N.113-118	N.N.N.119
	N.N.N.120	N.N.N.121-126	N.N.N.127
	N.N.N.128	N.N.N.129-134	N.N.N.135
	N.N.N.136	N.N.N.137-142	N.N.N.143
	N.N.N.144	N.N.N.145-150	N.N.N.151
	N.N.N.152	N.N.N.153-158	N.N.N.159
	N.N.N.160	N.N.N.161-166	N.N.N.167
	N.N.N.168	N.N.N.169-174	N.N.N.175
	N.N.N.176	N.N.N.177-182	N.N.N.183
	N.N.N.184	N.N.N.185-190	N.N.N.191
	N.N.N.192	N.N.N.193-198	N.N.N.199
	N.N.N.200	N.N.N.201-206	N.N.N.207
	N.N.N.208	N.N.N.209-214	N.N.N.215
	N.N.N.216	N.N.N.217-222	N.N.N.223
	N.N.N.224	N.N.N.225-230	N.N.N.231

	Network Number	Hosts Available	Broadcast Address
	N.N.N.232	N.N.N.233-238	N.N.N.239
	N.N.N.240	N.N.N.241-246	N.N.N.247
	N.N.N.248	N.N.N.249-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.252	N.N.N.0	N.N.N.1-2	N.N.N.3
/30	N.N.N.4	N.N.N.5-6	N.N.N.7
	N.N.N.8	N.N.N.9-10	N.N.N.11
	N.N.N.12	N.N.N.13-14	N.N.N.15
	N.N.N.16	N.N.N.17-18	N.N.N.19
	N.N.N.20	N.N.N.21-22	N.N.N.23
	N.N.N.24	N.N.N.25-26	N.N.N.27
	N.N.N.28	N.N.N.29-30	N.N.N.31
	N.N.N.32	N.N.N.33-34	N.N.N.35
	N.N.N.36	N.N.N.37-38	N.N.N.39
	N.N.N.40	N.N.N.41-42	N.N.N.43
	N.N.N.44	N.N.N.45-46	N.N.N.47
	N.N.N.48	N.N.N.49-50	N.N.N.51
	N.N.N.52	N.N.N.53-54	N.N.N.55
	N.N.N.56	N.N.N.57-58	N.N.N.59
	N.N.N.60	N.N.N.61-62	N.N.N.63
	N.N.N.64	N.N.N.65-66	N.N.N.67
	N.N.N.68	N.N.N.69-70	N.N.N.71
	N.N.N.72	N.N.N.73-74	N.N.N.75
	N.N.N.76	N.N.N.77-78	N.N.N.79
	N.N.N.80	N.N.N.81-82	N.N.N.83
	N.N.N.84	N.N.N.85-86	N.N.N.87
	N.N.N.88	N.N.N.89-90	N.N.N.91
	N.N.N.92	N.N.N.93-94	N.N.N.95
	N.N.N.96	N.N.N.97-98	N.N.N.99
	N.N.N.100	N.N.N.101-102	N.N.N.103
	N.N.N.104	N.N.N.105-106	N.N.N.107
	N.N.N.108	N.N.N.109-110	N.N.N.111
	N.N.N.112	N.N.N.113-114	N.N.N.115
	N.N.N.116	N.N.N.117-118	N.N.N.119
	N.N.N.120	N.N.N.121-122	N.N.N.123
	N.N.N.124	N.N.N.125-126	N.N.N.127
	N.N.N.128	N.N.N.129-130	N.N.N.131
	N.N.N.132	N.N.N.133-134	N.N.N.135
	N.N.N.136	N.N.N.137-138	N.N.N.139
	N.N.N.140	N.N.N.141-142	N.N.N.143
	N.N.N.144	N.N.N.145-146	N.N.N.147
	N.N.N.148	N.N.N.149-150	N.N.N.151
	N.N.N.152	N.N.N.153-154	N.N.N.155
	N.N.N.156	N.N.N.157-158	N.N.N.159
	N.N.N.160	N.N.N.161-162	N.N.N.163
	N.N.N.164	N.N.N.165-166	N.N.N.167
	N.N.N.168	N.N.N.169-170	N.N.N.171
	N.N.N.172	N.N.N.173-174	N.N.N.175
	N.N.N.176	N.N.N.177-178	N.N.N.179
	N.N.N.180	N.N.N.181-182	N.N.N.183
	N.N.N.184	N.N.N.185-186	N.N.N.187
	N.N.N.188	N.N.N.189-190	N.N.N.191
	N.N.N.192	N.N.N.193-194	N.N.N.195
	N.N.N.196	N.N.N.197-198	N.N.N.199
	N.N.N.200	N.N.N.201-202	N.N.N.203
	N.N.N.204	N.N.N.205-206	N.N.N.207
	N.N.N.208	N.N.N.209-210	N.N.N.211
	N.N.N.212	N.N.N.213-214	N.N.N.215
	N.N.N.216	N.N.N.217-218	N.N.N.219
	N.N.N.220	N.N.N.221-222	N.N.N.223
	N.N.N.224	N.N.N.225-226	N.N.N.227
	N.N.N.228	N.N.N.229-230	N.N.N.231
	N.N.N.232	N.N.N.233-234	N.N.N.235
	N.N.N.236	N.N.N.237-238	N.N.N.239
	N.N.N.240	N.N.N.241-242	N.N.N.243
	N.N.N.244	N.N.N.245-246	N.N.N.247
	N.N.N.248	N.N.N.249-250	N.N.N.251
	N.N.N.252	N.N.N.253-254	N.N.N.255

Appendix B – Wireless Antenna

GSM/EGSM Antenna Requirements/Specifications

Frequency Range:	824 – 960 MHz / 1710 – 1990 MHz
Impedance:	50 Ohms
VSWR:	<2.0:1
Typical Radiated Gain:	3 dBi on azimuth plane
Radiation:	Omni
Polarization:	Vertical
Wave:	Half Wave Dipole

Antennas Available from Multi-Tech Systems, Inc.

Description	Part Number
Hinged Right Angle 900/1800 MHz Cellular Modem Antenna	ANF1-1HRA
Hinged Right Angle 800/1900 MHz Cellular Modem Antenna	ANF21HRA
Hinged Right Angle 850/900/1800/1900 MHz Cellular Modem Antenna	ANQB-1HRA

PTCRB Requirements Note:

There cannot be any alteration to the authorized antenna system. The antenna system must be the same type with similar in-band and out-of-band radiation patterns and maintain the same specifications.

FCC Requirements Note:

The antenna gain, including cable loss, must not exceed 3.0 dBi at 1900 MHz / 1.6 dBi at 850 MHz for mobile operating configurations and 7.0 dBi at 1900 MHz / 2.3 dBi at 850 MHz for fixed mounted operations, as defined in 2.1091 and 1.1307 of the rules for satisfying RF exposure compliance.

GSM and E-GSM Radio Characteristics

	GSM 850	E-GSM 900	GSM 1800	GSM 1900
Frequency RX	869 to 894 MHz	925 to 960 MHz	1805 to 1880 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz
RF Power Stand	2W at 12.5% duty cycle	2W at 12.5% duty cycle	1W at 12.5% duty cycle	1W at 12.5% duty cycle
Impedance	50 ohms			
VSWR	<2			
Typical Radiated Gain	0 dBi on azimuth plane			

Appendix C – Regulatory Compliance

CE

EMC, Safety, and R&TTE Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 2004/108/EC of 15 December 2004 on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 2006/95/EC of 12 December 2006 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

FCC Part 15 Class A Statement

This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to 47 CFR Part 15 regulations. The stated limits in this regulation are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Plug the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the CFR 47 rules. Operation of this device is subject to the following conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement Canadien sur le matériel brouilleur.

Appendix D – Waste Electrical and Electronic Equipment

July, 2005

Waste Electrical and Electronic Equipment (WEEE)

The WEEE directive places an obligation on EU-based manufacturers, distributors, retailers and importers to take-back electronics products at the end of their useful life. A sister Directive, ROHS (Restriction of Hazardous Substances) complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all Multi-Tech products imported into the EU as of August 13, 2005. EU-based manufacturers, distributors, retailers and importers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging, which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of their waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or where you purchased the product.

Appendix C – ROHS HT/TS Substance Concentration

依照中国标准的有毒有害物质信息

根据中华人民共和国信息产业部 (MII) 制定的电子信息产品 (EIP) 标准－中华人民共和国《电子信息产品污染控制管理办法》（第 39 号），也称作中国 RoHS，下表列出了 Multi-Tech Systems Inc. 产品中可能含有的有毒物质 (TS) 或有害物质 (HS) 的名称及含量水平方面的信息。

成分名称	有害/有毒物质/元素					
	铅 (PB)	汞 (Hg)	镉 (CD)	六价铬 (CR6+)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板	O	O	O	O	O	O
电阻器	X	O	O	O	O	O
电容器	X	O	O	O	O	O
铁氧体磁环	O	O	O	O	O	O
继电器/光学部件	O	O	O	O	O	O
IC	O	O	O	O	O	O
二极管/晶体管	O	O	O	O	O	O
振荡器和晶振	X	O	O	O	O	O
调节器	O	O	O	O	O	O
电压传感器	O	O	O	O	O	O
变压器	O	O	O	O	O	O
扬声器	O	O	O	O	O	O
连接器	O	O	O	O	O	O
LED	O	O	O	O	O	O
螺丝、螺母以及其它五金件	X	O	O	O	O	O
交流-直流电源	O	O	O	O	O	O
软件/文档 CD	O	O	O	O	O	O
手册和纸页	O	O	O	O	O	O
底盘	O	O	O	O	O	O

X 表示所有使用类似材料的设备中有害/有毒物质的含量水平高于 SJ/Txxx-2006 限量要求。

O 表示不含该物质或者该物质的含量水平在上述限量要求之内

Index

A

Access Point Name 19
AH Key 47
Authentication Algorithms 47
Auto Dialout configuration 23
Autodiscovery configuration 23

B

Broadcast timer 23
Browse File for Upgrade in Tools 52
Browse File to Load Configuration 53

C

Caller ID for Wakeup on Call 30
Canadian Regulations 63
Checking Network Registration 16
Checking Roaming Status 16
Configure Ethernet interface 17

D

Daylight Savings Time configuration 26
DDNS Client 25
DDNS configuration 25
DDNS Status in Tools 52
DHCP configuration 42
DHCP fixed addresses 43
DHCP Lease Time 42
DHCP server 42
Dial-on-Demand 29
DNAT configuration 37
DNAT example 37
Dynamic DNS configuration 25

E

EMC, Safety, and R&TTE Directive Compliance 63
Ethernet ports caution 6
Exiting Modem Mode 16

F

Firmware Upgrade 52

G

General Configuration – IP Setup 22
GRE route configuration 41
GRE routing 40
GRE tunnel configuration 40
GRE tunneling 40

H

H323 packets connection tracking 39
Handling Precautions 6
HTTP authentication 24
HTTP configuration 24

I

ICMP configuration 39
ICMP Keep Alive Check 29
International Modem Restrictions 63
IP Configuration 23
IP Server 25
ITCP 35

L

Load Configuration 53

M

Menu structure 20
Modem Information 60, 61

N

NAT configuration 28
Navigating 20
Network configuration 34
Network/Host for Remote Configuration 27

O

Operating Temperature 9

P

Packet Filter 36
Packet filter rules 36
Perfect Forward Secrecy 45
Pin Functions 10
Polling time 26
Power-On Configuration 33
PPP authentication 29
PPP configuration 29
PPTP connection tracking 39
protocol 35

R

Raw Dialout configuration 23
Remote Configuration 27
Reset Modem in Tools 52
Route configuration 27

S

Safe password 24
Save configuration in Tools 53
Screen parts 21
Select encryption method 47

Server Port 23
Service Configuration 35
Shutdown caution 19
SNTP configuration....26
Static Routes configuration 27
Statistics & Logs > DHCP Statistics....57
Statistics & Logs > Ethernet....55
Statistics & Logs > Modem Information 58
Statistics & Logs > PPP....56
Sub-menus 21
Subnets....60
Supported Subnets....60
Syslog configuration 23
System domain name....25

T

Time zone configuration 26
Tools....52

U

UDP 35

V

Vehicle Safety....6

W

Wakeup on Call 30
Wakeup on Call Examples 31, 32
Wizard Setup....17, 18